Carnegie Mellon
Software Engineering Institute

Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Framework, Version 1.0

Christopher J. Alberts
Sandra G. Behrens
Richard D. Pethia
William R. Wilson

June 1999

TECHNICAL REPORT
CMU/SEI-99-TR-017
ESC-TR-99-017

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of "Don't ask, don't tell, don't pursue" excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Framework, Version 1.0

CMU/SEI-99-TR-017
ESC-TR-99-017

Christopher J. Alberts
Sandra G. Behrens
Richard D. Pethia
William R. Wilson

June 1999

Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Norton L Compton

Norton L. Compton, Lt Col., USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

Acknowledgments

The authors would like to acknowledge the following individuals for their contributions to this document: Julia Allen, Suresh Konda, and Brad Willke for their contributions as members of the development team; Linda Pesante for editing the content of the document; Bill Thomas for providing the copy edit for the document.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM})[*] is a framework for identifying and managing information security risks. It defines a comprehensive evaluation method that allows an organization to identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. With this understanding, the organization can design and implement a protection strategy to reduce the overall risk exposure of its information assets.

[*] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

1 Introduction

The Networked Systems Survivability (NSS) Program of the Software Engineering Institute (SEI) has begun developing the Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM})* framework to describe an information security risk evaluation. OCTAVE defines a set of self-directed activities for organizations to identify and manage their information security risks. Evaluations that are consistent with the OCTAVE framework will be comprehensive and will allow an organization to identify the information assets that are important to its mission, the threats to those assets, and the vulnerabilities that may expose those information assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. Once it has a picture of the risks, the organization can design a protection strategy to reduce the overall risk exposure of its information assets.

This document describes the essential components of OCTAVE, focusing on what each process step accomplishes. Issues such as who will perform the steps or how to perform them will be addressed in subsequent publications. By issuing this report, we intend to initiate a discussion of what elements make up a comprehensive information security risk assessment that examines both organizational and technology issues. Over time, as we develop and pilot an evaluation method consistent with the OCTAVE framework, we anticipate that the details described in this report will be modified. When appropriate, we will revise this document and the method to reflect changes based on comments from the community as well as on our field experience.

The current version of OCTAVE comes primarily from the following three sources:

- Information Security Evaluation (ISE). The ISE is an information security vulnerability evaluation developed by the Software Engineering Institute's Networked Systems Survivability Program. It focuses on identifying vulnerabilities in an organization's computing infrastructure. It addresses assets and threats implicitly. OCTAVE developers are incorporating the lessons learned from the development and delivery of the ISE into the OCTAVE framework and method.
- Software risk management expertise. OCTAVE is also incorporating many of the diagnostic techniques and theories developed by the SEI's Risk Program, which focused on identifying risks to software development projects. Many of the principles for OCTAVE's Phase 1 are derived from work that focused on risk management issues facing managers in a software development organization.

* Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

- Surveying the current state of the practice in information security risk management. Articles about state-of-the-practice information security assessments were examined prior to the development of OCTAVE. This information was used to determine what is working in the community and where the community could benefit from a self-directed comprehensive information security risk assessment.

1.1 The Need for OCTAVE

Information systems are essential to most organizations today. The integrity, availability, and confidentiality of information are critical to organizations' missions. However, few organizations focus on their most important information assets when they make decisions about protecting their information. For example, a bank might consider its customers' bank records to be one of its important information assets. Likewise, a military organization responsible for deploying troops might consider logistical data to be an important information asset. Most organizations form their protection strategies by focusing solely on infrastructure weaknesses. Those organizations fail to establish the effect of the infrastructure weaknesses on information assets, such as bank records or logistical data.

This leads to a gap between the organization's operational requirements and information technology (IT) requirements. Often, the computing infrastructure is set up without the IT staff having a clear understanding of the organization's mission- or business-related needs. It is not clear if important information is being adequately protected. Likewise, significant effort might be directed toward protecting relatively unimportant information. In these situations, the operational or business units of the organization and the information technology department are not communicating effectively.

Often, information protection decisions are made in an ad hoc manner, based on the IT department's prior experience with vulnerabilities and the threats that they currently know about. Thus, risks tend not to be systematically managed or are managed by the wrong people.

Most current approaches to information-security risk management tend to be incomplete, expert-driven, or both. Most approaches fail to include all the components of information security risk (assets, threats, and vulnerabilities). In these cases, the organization has insufficient data to fully match a protection strategy to its security risks.

Many organizations outsource information security risk assessments because they do not have in-house capability to perform this vital service. They hire experts to perform risk assessments, and the resulting assessment is only as good as the experts who perform it. Often the consumers of such services have no way to understand if the risk assessment performed for them is adequate for their enterprise.

OCTAVE enables organizations to avoid those problems. It defines the essential components of a systematic information-security risk assessment. By following the OCTAVE framework, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information assets. The operational or business units and the departments responsible for the information infrastructure work together to address the information security needs of the enterprise. OCTAVE thus gives the organization a comprehensive, systematic, context-driven approach to managing information-security risks.

1.2 Overview of OCTAVE

OCTAVE examines organizational issues and technology issues to assemble a comprehensive picture of the information security needs of an enterprise. It contains the following phases:

- Phase 1, Build Enterprise-Wide Security Requirements
- Phase 2, Identify Infrastructure Vulnerabilities
- Phase 3, Determine Security Risk Management Strategy

Each phase of OCTAVE is designed to produce meaningful results for the organization.

During Phase 1, information assets and their values, threats to those assets, and security requirements are identified using knowledge of the staff from multiple levels within the organization, along with standard catalogs of information. For example, known threat profiles and good organizational and technical practices are used to probe staff members for their knowledge of the organization's assets, threats, and current protection strategies. This information can then be used to establish the security requirements of the enterprise, which is the goal of the first phase of OCTAVE.

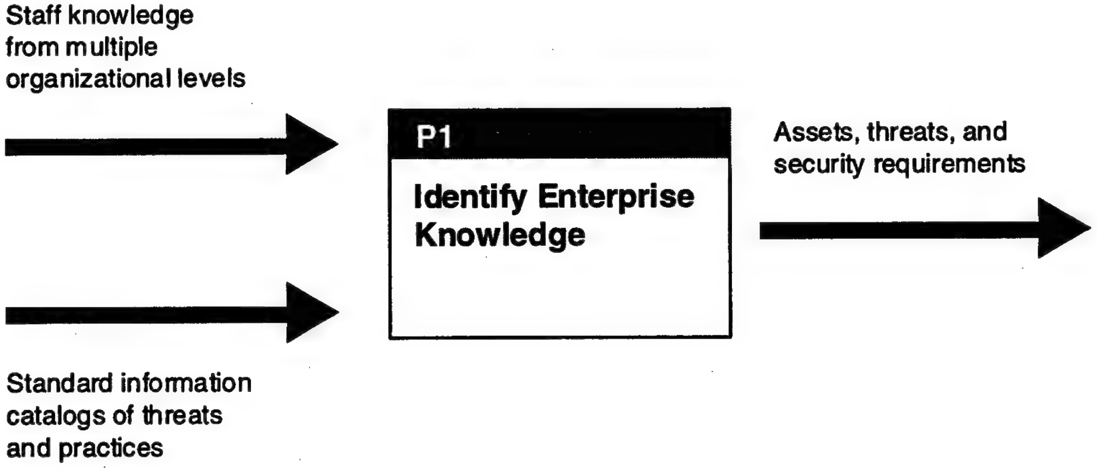

Staff knowledge from multiple organizational levels
P1
Identify Enterprise Knowledge
Assets, threats, and security requirements
Standard information catalogs of threats and practices

Figure 1: OCTAVE Phase 1, Build Enterprise-Wide Security Requirements

Phase 2 of OCTAVE builds on the information captured during Phase 1 by mapping the information assets of the organization to the information infrastructure components (both the physical environment and networked IT environment) to identify the high-priority infrastructure components. Once this is done, an infrastructure vulnerability evaluation is performed to identify vulnerabilities. As in Phase 1, standard catalogs of information are used; for example, standard intrusion scenarios and vulnerability information are used as a basis for the infrastructure vulnerability evaluation. At the conclusion of Phase 2, the organization has identified the high-priority information infrastructure components, missing policies and practices, and vulnerabilities.

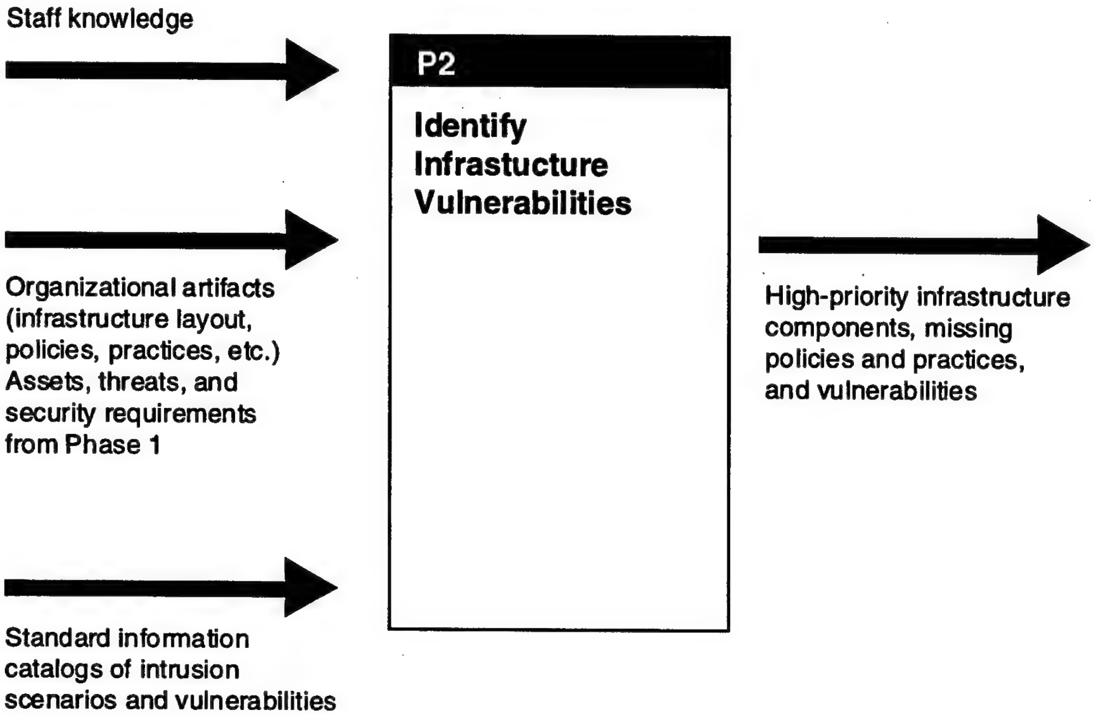

Staff knowledge
P2
Identify Infrastucture Vulnerabilities
Organizational artifacts (infrastructure layout, policies, practices, etc.) Assets, threats, and security requirements from Phase 1
Standard information catalogs of intrusion scenarios and vulnerabilities
High-priority infrastructure components, missing policies and practices, and vulnerabilities

Figure 2: OCTAVE Phase 2, Identify Infrastructure Vulnerabilities

Phase 3 of OCTAVE builds on the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities identified in OCTAVE's earlier phases in the context of standard intrusion scenarios. The impact and probability of the risks (also called the risk attributes) are estimated and subsequently used to help prioritize the risks. The prioritized list of risks is used in conjunction with information from the previous phases to develop a protection strategy for the enterprise and to establish a comprehensive plan for managing security risks, which are among the goals of Phase 3.

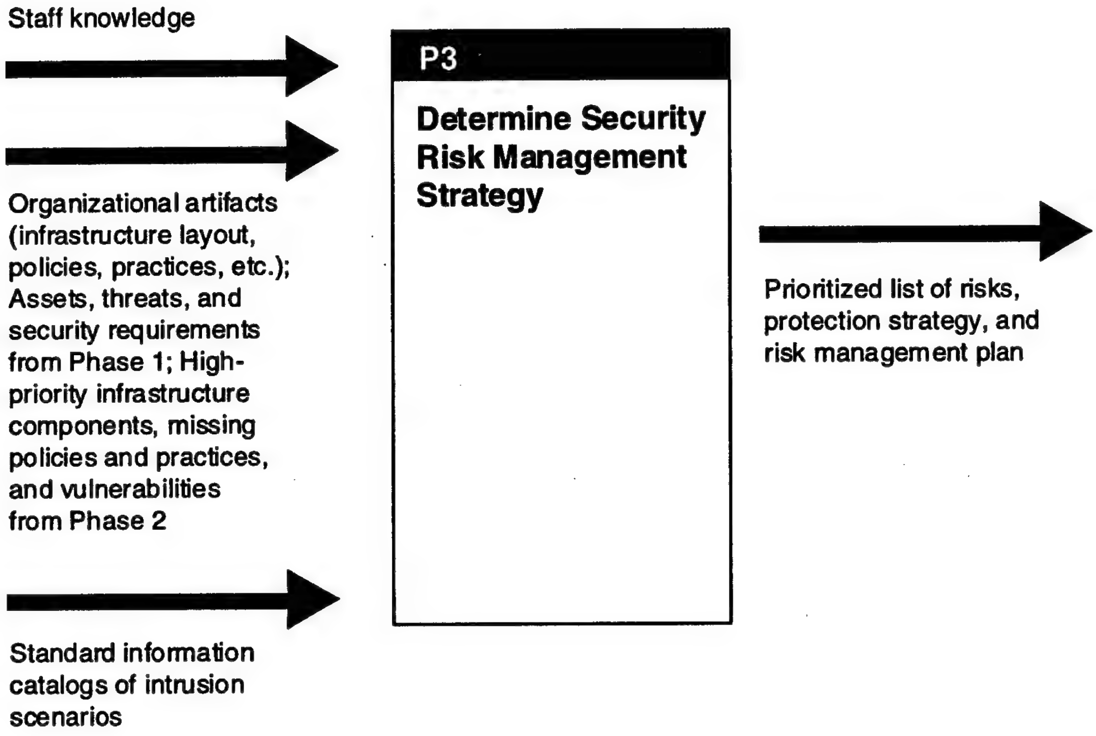

Staff knowledge
Organizational artifacts (infrastructure layout, policies, practices, etc.); Assets, threats, and security requirements from Phase 1; High-priority infrastructure components, missing policies and practices, and vulnerabilities from Phase 2
Standard information catalogs of intrusion scenarios
P3
Determine Security Risk Management Strategy
Prioritized list of risks, protection strategy, and risk management plan

Figure 3: OCTAVE Phase 3, Determine Security Risk Management Strategy

1.3 Example Scenario

To illustrate how using OCTAVE can help an enterprise understand its information security risks, consider the following example. An enterprise with sensitive financial information is interested in understanding and addressing its information security risks. The enterprise's management is concerned that outsiders could have access to financial information that could be used for illegal stock trading. The senior managers decide to perform a security assessment to understand its risk in this area.

An outside consulting firm is hired to evaluate the enterprise's security. The following observations are among those identified by the consultants:

- The enterprise's firewall is functioning correctly—outsiders would have a hard time getting in.
- There are no back doors into the network.
- The number of accounts on most servers is limited.
- Most servers are accessed remotely.
- Authentication is required when users access servers.
- There is one vulnerability: user IDs and passwords travel across the network in clear text.

The consultants failed to develop a picture of the risk facing the enterprise. Consequently, senior managers believed that the financial information was secure, based on the results of the assessment. They felt safe from the threat of outsiders breaking into their network and stealing sensitive financial information. They were not considering other potential threats.

Consider a second evaluation, which is performed by following the OCTAVE framework. Personnel from senior management, middle management, and staff levels participated in the risk evaluation. Phase 1 of OCTAVE was performed to identify assets, threats, and security requirements.

One of the most critical assets identified was the sensitive financial information. If this information were made public, the reputation of the enterprise would suffer and could result in millions of dollars of lost business. In addition, anyone knowing this information could use it to profit illegally by trading stocks. The relative impact of losing the confidentiality of this information was high. Thus, one of the security requirements for the financial information was that it must be confidential.

OCTAVE requires participants to consider a variety of potential threats. (The term "threats" indicates what or whom the assets are being protected from.) Several threats had motivation to possess this information, because the information could be used for financial gain. Furthermore, it was determined that the threats could be insiders or outsiders. One possible means for threats to gain access to the information was via the network, and all employees had access to the network. Technically savvy employees might be able to exploit any vulnerabilities that might be present.

In addition, the information supplied by staff-level employees indicated that there was some dissatisfaction among some of the technical employees in the company. Thus, disgruntled insiders might have both the motive and the means to steal the information.

Next, Phase 2 of OCTAVE was performed to identify infrastructure vulnerabilities. First, the important infrastructure components were identified through an examination of the layout of the physical and IT infrastructures. Because sensitive financial information was an important information asset, the server that contained the database with that information was identified as a high-priority component. A vulnerability evaluation for the server was performed.

The vulnerability evaluation indicated the following:

- The number of accounts on the server holding the sensitive information is limited.
- The server is accessed remotely.
- Authentication is required when a user accesses the server.
- There was one major vulnerability: user IDs and passwords travel across the network in clear text.

Phase 3 of OCTAVE calls for an analysis of the asset, threat, and vulnerability information identified during Phases 1 and 2, in the context of intrusion scenarios to identify the organization's risks. For example, the following intrusion scenario can be built using the information in this example:

> *A technically savvy, disgruntled insider uses a network sniffer to steal passwords to the server containing the sensitive database. As soon as a password is known, the insider can access the sensitive information and use it for personal gain or make it public.*
>
> *The likelihood of such an attack was judged to be moderate to high. The impact would be high in terms of damage to the company's reputation. This was judged to be a big risk to the enterprise.*

The senior managers understood the nature of this risk. They understood that it was possible for a sufficiently motivated insider to steal sensitive financial information and use it for profit. This was only one of many such risks to be identified using OCTAVE. The enterprise staff was now ready to start developing a strategy to protect the sensitive financial information as well as other important assets.

By performing a comprehensive risk assessment that considers asset, threat, and vulnerability information and puts it into the context of the enterprise, the risks facing the enterprise can be identified. In addition, personnel from all levels can understand risks when they are put into the context of the enterprise, and can make sensible decisions concerning a protection strategy.

1.4 Report Overview

In the rest of this report, OCTAVE will be outlined in detail. We will describe each of the three phases of OCTAVE and the multiple processes within each phase. For each OCTAVE process, we include the following:

- process activities—a high-level description of what happens at each step of the process. Included with the description of each activity is a description of the inputs and outputs of each process.

- process diagram—a data-flow diagram showing the inputs and outputs of the process

Following the phase and process descriptions are higher-level views of OCTAVE. Section 5 concisely summarizes OCTAVE goals and processes. The appendix provides a flowchart of the OCTAVE method.

2 Phase 1: Build Enterprise-Wide Security Requirements

Phase 1 of OCTAVE is named "Build Enterprise-Wide Security Requirements" and has four processes. This phase examines the enterprise by eliciting information from people within the organization. Staff members from multiple levels of the organization participate, contributing their unique perspectives and knowledge. Standard catalogs of information about organizational and technical practices and threats are used as a basis for probing the staff members about their perspectives. The ultimate goal of Phase 1 is to establish the security requirements of the enterprise.

Process 1 examines the senior management or enterprise perspective; Process 2 examines the middle management or operational area perspective; and Process 3 examines the perspective of the staff level of the enterprise. Each process identifies what the participants perceive to be the key assets, the threats to those assets, and the current protection strategy employed by the enterprise. Any concerns or indications of risk are also captured during each of these three processes. The final process of Phase 1, Process 4, integrates the individual perspectives to produce an enterprise view of the assets, threats, protection strategies, and risk indicators. In addition, Process 4 produces the security requirements necessary to provide confidentiality, integrity, and/or availability of the key information assets.

The following four processes comprise Phase 1 of OCTAVE:

- Process 1, Identify Enterprise Knowledge. This process identifies what senior managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.

- Process 2, Identify Operational Area Knowledge. This process identifies what operational area managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.

- Process 3, Identify Staff Knowledge. This process identifies what staff-level personnel perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise

- Process 4, Establish Security Requirements. This process integrates the individual perspectives identified in the first three processes to produce an enterprise view of the assets, threats, protection strategies, and risk indicators. In addition, the security requirements of the enterprise are identified.

We will examine each of these processes in the following sections.

2.1 Process 1: Identify Enterprise Knowledge

OCTAVE's first process, Identify Enterprise Knowledge, defines the activity of eliciting knowledge about important assets, threats, and protection strategies from the people holding senior management positions.

The goal of this process is to understand the perspective of senior managers within the enterprise. Subsequent process steps examine the same issues from the perspective of personnel at other levels within the organization. The following sections examine the activities and provide an input/output diagram for Process 1.

2.1.1 Activities

Inputs for this process include both what the participants contribute to the process (their knowledge and perspectives) and artifacts required by the process (such as standard catalogs of information). Outputs of this process are tangible artifacts that capture the knowledge and perspectives of the participants. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 2 are the following:

1. **Characterize key enterprise assets**—elicits and prioritizes the key assets in the organization from the perspective of senior management. These are the assets that senior managers would most like to protect. This part of the process answers the following question:

   - What are you trying to protect?

   This activity uses the following inputs:

   - *Current knowledge of senior managers (I1.1)*—the knowledge of senior managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Asset questionnaire (I1.2)*—an instrument designed to elicit information about important assets.

   This activity produces the following output:

   - *Prioritized list of enterprise assets with relative values (O1.1)*—a prioritized ordering of important assets and their relative values from the perspective of senior management.

2. **Describe threats to assets**—elicits a description of the threats to the identified assets in the organization from the perspective of senior management. Threats indicate what or

whom the assets are being protected from. This part of the process answers the following question:

- What are you trying to protect your assets from?

This activity uses the following inputs:

- *Current knowledge of senior managers (I1.1)*—the knowledge of senior managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.
- *Generic threat profile (I1.3)*—an instrument designed to elicit information about threats to important assets. The threat profile is created by incorporating a catalog of threats, which is a standard compilation of known threat data.

This activity produces the following output:

- *Enterprise threat profile (O1.2)*—the threats to enterprise assets from the perspective of senior management.

3. **Describe current and planned strategy to protect assets**—elicits senior management's knowledge of the policies and practices—both current and planned—to protect the identified assets. The protection strategy outlines what is being done to protect the enterprise's important information assets. This part of the process answers the following question:

   - What are you currently doing to protect your assets?

   This activity uses the following inputs:

   - *Current knowledge of senior managers (I1.1)*—the knowledge of senior managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.
   - *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:
     - catalog of organization practices—a standard compilation of known good organizational practices
     - catalog of technical practices—a standard compilation of known good technical practices

    - catalog of training practices—a standard compilation of known good training practices

- *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

- *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

This activity produces the following output:

- *Current enterprise protection strategy (O1.3)*—the enterprise's current or planned protection strategy from the perspective of senior management.

4. **Identify risk indicators**—elicits senior management's knowledge of known gaps in the current protection strategy. Risk indicators are typically organizational issues. Examples include not having an adequate security training and awareness program for the staff and not having documented policies and procedures for protecting information assets. This part of the process answers the following question:

- What gaps in your current protection strategy are putting your assets at risk?

This activity uses the following inputs:

- *Current knowledge of senior managers (I1.1)*—the knowledge of senior managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

- *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:

    - catalog of organization practices—a standard compilation of known good organizational practices

    - catalog of technical practices—a standard compilation of known good technical practices

    - catalog of training practices—a standard compilation of known good training practices

- *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

- *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

This activity produces the following output:

- *Enterprise risk indicators (O1.4)*—concerns expressed by senior management indicating that there is a potential for assets to be at risk.

5. **Select operational areas to evaluate**—elicits the operational areas that should participate in the evaluation. Managers and key staff to participate in the process are also identified. Operational areas are at the level below the senior managers in the organization (a business unit would be a key operational area). Operational areas can include support functions, such as business development, marketing, and information technology activities. This part of the process requires using information gathered in the previous four steps in addition to senior management's knowledge. It answers the following questions:

   - What operational areas or support functions are involved with the key assets that you identified?

   - Who are the key managers of those operational areas or support functions?

   This activity uses the following inputs:

   - *Current knowledge of senior managers (I1.1)*—the knowledge of senior managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

   This activity produces the following output:

   - *Operational areas to evaluate (O1.5)*—key operational areas (those affecting the highest priority enterprise assets) to be examined in the evaluation as well as managers and key staff of those areas.

2.1.2 Diagram

The following is the process diagram of Process 1. The diagram highlights the inputs and outputs to the process.

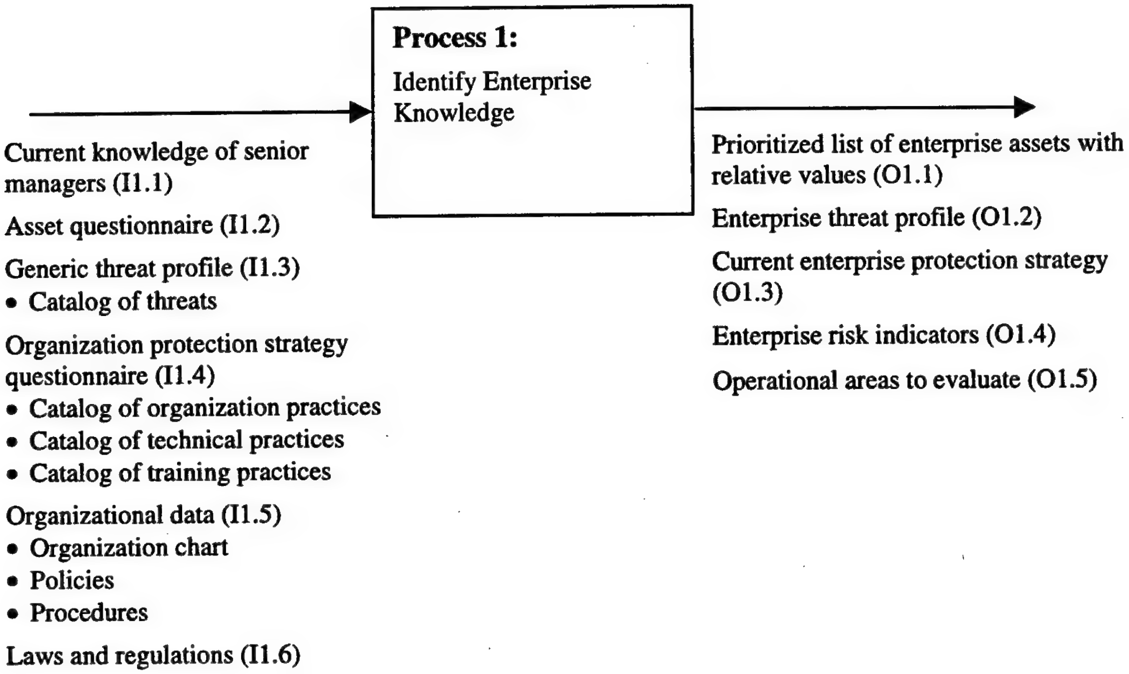

Process 1:
Identify Enterprise Knowledge
Current knowledge of senior managers (I1.1)
Asset questionnaire (I1.2)
Generic threat profile (I1.3)
• Catalog of threats
Organization protection strategy questionnaire (I1.4)
• Catalog of organization practices
• Catalog of technical practices
• Catalog of training practices
Organizational data (I1.5)
• Organization chart
• Policies
• Procedures
Laws and regulations (I1.6)
Prioritized list of enterprise assets with relative values (O1.1)
Enterprise threat profile (O1.2)
Current enterprise protection strategy (O1.3)
Enterprise risk indicators (O1.4)
Operational areas to evaluate (O1.5)

Figure 4: OCTAVE Process 1, Identify Enterprise Knowledge

2.2 Process 2: Identify Operational Area Knowledge

OCTAVE's second process, Identify Operational Area Knowledge, defines the activity of eliciting knowledge about important assets, threats, and protection strategies from the people who manage operational areas. An example of an operational area in some organizations would be a business unit.

The goal of this process is to understand the perspective of operational area managers within the enterprise. Other OCTAVE processes examine the same issues from the perspective of other levels within the enterprise. The following sections examine the activities and provide an input/output diagram for Process 2.

2.2.1 Activities

Inputs for this process include both what the participants contribute to the process (their knowledge and perspectives) and artifacts required by the process (such as standard catalogs of information). Outputs of this process are tangible artifacts that capture the knowledge and perspectives of the participants. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 2 are the following:

1. **Characterize key operational area assets**—elicits and prioritizes the key assets in the organization from the perspective of operational area management. These are the assets that operational area managers would most like to protect. This part of the process answers the following question:

   - What are you trying to protect?

   This activity uses the following inputs:

   - *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Asset questionnaire (I1.2)*—an instrument designed to elicit information about important assets.

   This activity produces the following output:

   - *Prioritized list of operational area assets with values (O2.1)*—a prioritized ordering of important assets and their relative values from the perspective of operational area management.

2. **Characterize assets in relation to enterprise assets**—elicits existing relationships between the operational area assets identified in the previous activity with the enterprise assets identified in Process 1. This part of the process answers the following question:

   - What are the relationships between the assets you have identified and the enterprise assets identified by senior management?

   This activity uses the following inputs:

   - *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Prioritized list of enterprise assets with relative values (O1.1)*—a prioritized ordering of important assets and their relative values from the perspective of senior management.

   - *Prioritized list of operational area assets with values (O2.1)*—a prioritized ordering of important assets and their relative values from the perspective of operational area management.

   This activity produces the following output:

   - *Operational area asset/enterprise asset map (O2.2)*—documented relationships or mapping between operational area assets and enterprise assets.

3. **Describe threats to assets**—elicits a description of the threats to the identified assets in the organization from the perspective of operational area management. Threats indicate what or whom the assets are being protected from. This part of the process answers the following question:

   - What are you trying to protect your assets from?

   This activity uses the following inputs:

   - *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Generic threat profile (I1.3)*—an instrument designed to elicit information about threats to important assets. The threat profile is created by incorporating a catalog of threats, which is a standard compilation of known threat data.

This activity produces the following output:

- *Operational area threat profile (O2.3)*—the threats to operational area assets from the perspective of operational area management.

4. **Describe current and planned strategy to protect assets**—elicits operational area management's knowledge of the policies and practices—both current and planned—to protect the identified assets. The protection strategy outlines what is being done to protect the operational area's important information assets. This part of the process answers the following question:

   - What are you currently doing to protect your assets?

   This activity uses the following inputs:

   - *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:

     - catalog of organization practices—a standard compilation of known good organizational practices

     - catalog of technical practices—a standard compilation of known good technical practices

     - catalog of training practices—a standard compilation of known good training practices

   - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

   - *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

   This activity produces the following output:

   - *Current operational area protection strategy (O2.4)*—the operational area's current or planned protection strategy from the perspective of operational area management.

5. **Identify risk indicators**—elicits operational area management's knowledge of known gaps in the current protection strategy. Risk indicators are typically organizational issues. Examples include not having an adequate security training and awareness program for the staff and not having documented policies and procedures for protecting information assets. This part of the process answers the following question:

   - What gaps in your current protection strategy are putting your assets at risk?

   This activity uses the following inputs:

   - *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:

     - catalog of organization practices—a standard compilation of known good organizational practices

     - catalog of technical practices—a standard compilation of known good technical practices

     - catalog of training practices—a standard compilation of known good training practices

   - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

   - *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

   This activity produces the following output:

   - *Operational area risk indicators (O2.5)*—concerns expressed by operational area management indicating that there is a potential for assets to be at risk.

6. **Select staff to evaluate**—elicits which staff should participate in the evaluation. This requires using information gathered in the previous four steps in addition to operational area management's knowledge. The staff level of an organization defines the level below the operational area (a project leader would be a key staff member). The staff levels can

also include support functions, such as business development, marketing, and information technology activities. This part of the process answers the following questions:

- What projects or support functions are involved with the key assets that you identified?

- Who are the key staff members of those projects or support functions?

This activity uses the following inputs:

- *Current knowledge of operational area managers (I2.1)*—the knowledge of operational area managers concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

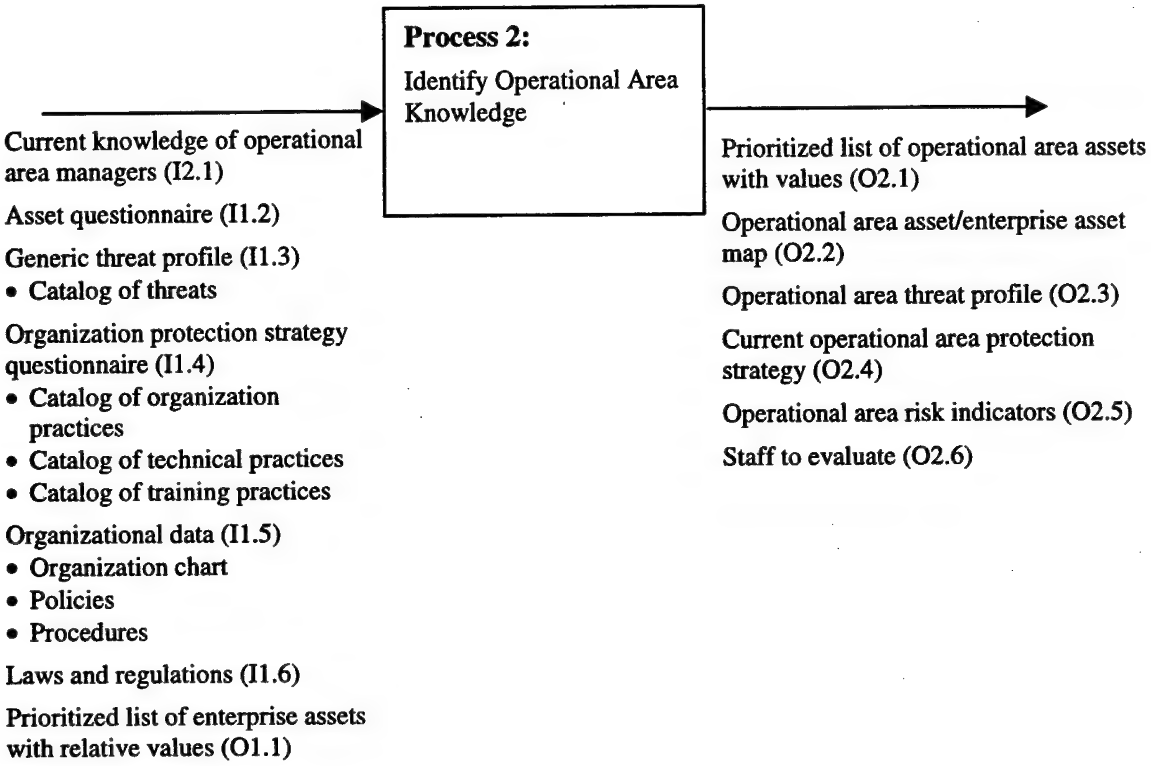
- *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

This activity produces the following output:

- *Staff to evaluate (O2.6)*—key staff (those affecting the highest priority operational area assets). This can include project and support function team leaders as well as key project and support function team members.

2.2.2 Diagram

The following is the process diagram of Process 2. The diagram highlights the inputs and outputs to the process.



Process 2:

Identify Operational Area Knowledge

Current knowledge of operational area managers (I2.1)

Asset questionnaire (I1.2)

Generic threat profile (I1.3)
- Catalog of threats

Organization protection strategy questionnaire (I1.4)
- Catalog of organization practices
- Catalog of technical practices
- Catalog of training practices

Organizational data (I1.5)
- Organization chart
- Policies
- Procedures

Laws and regulations (I1.6)

Prioritized list of enterprise assets with relative values (O1.1)

Prioritized list of operational area assets with values (O2.1)

Operational area asset/enterprise asset map (O2.2)

Operational area threat profile (O2.3)

Current operational area protection strategy (O2.4)

Operational area risk indicators (O2.5)

Staff to evaluate (O2.6)

Figure 5: OCTAVE Process 2, Identify Operational Area Knowledge

2.3 Process 3: Identify Staff Knowledge

OCTAVE's third process, Identify Staff Knowledge, defines the activity of eliciting knowledge about important assets, threats, and protection strategies from the people who work directly (project teams) or indirectly (support functions such as information technology or marketing) toward the mission of an organization.

The goal of this process is to understand the perspective of the staff within the enterprise. Other OCTAVE processes examine the same issues from the perspectives of other levels within the enterprise. The following sections examine the activities of Process 3 and provide an input/output diagram for this process.

2.3.1 Activities for Process 3: Identify Staff Knowledge

Inputs for this process include both what the participants contribute to the process (their knowledge and perspectives) and artifacts required by the process (such as standard catalogs of information). Outputs of this process are tangible artifacts that capture the knowledge and perspectives of the participants. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 3 are the following:

1. **Characterize key staff assets**—elicits and prioritizes the key assets in the organization from the staff's perspective. These are the assets that the staff would most like to protect. This part of the process answers the following question:

   - What are you trying to protect?

   This activity uses the following inputs:

   - *Current knowledge of staff (I3.1)*—the knowledge of the staff concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Asset questionnaire (I1.2)*—an instrument designed to elicit information about important assets.

   This activity produces the following output:

   - *Prioritized list of staff assets with values (O3.1)*—a prioritized ordering of important assets and their relative values from the staff's perspective.

2. **Characterize assets in relation to operational area and enterprise assets**—elicits existing relationships between the staff assets identified in the previous activity with the

operational area and enterprise assets identified in previous processes. This part of the process answers the following question:

- What are the relationships between the assets you have identified, the operational area assets identified by operational area management, and the enterprise assets identified by senior management?

This activity uses the following inputs:

- *Current knowledge of staff (I3.1)*—the knowledge of the staff concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.
- *Prioritized list of enterprise assets with relative values (O1.1)*—a prioritized ordering of important assets and their relative values from the perspective of senior management.
- *Prioritized list of operational area assets with values (O2.1)*—a prioritized ordering of important assets and their relative values from the perspective of operational area management.
- *Operational area asset/enterprise asset map (O2.2)*—documented relationships or mapping between operational area assets and enterprise assets.

This activity produces the following output:

- *Staff asset/operational area asset/enterprise asset map (O3.2)*—documented relationships or mapping among staff assets, operational area assets, and enterprise assets.

3. **Describe threats to assets**—elicits a description of the threats to the identified assets in the organization from the staff's perspective. Threats indicate what or whom the assets are being protected from. This part of the process answers the following question:

    - What are you trying to protect your assets from?

    This activity uses the following inputs:

    - *Current knowledge of staff (I3.1)*—the knowledge of the staff concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.
    - *Generic threat profile (I1.3)*—an instrument designed to elicit information about threats to important assets. The threat profile is created by incorporating a catalog of threats, which is a standard compilation of known threat data.

This activity produces the following output:

- *Staff threat profile (O3.3)*—the threats to staff assets from the staff's perspective.

4. **Describe current and planned strategy to protect assets**—elicits the staff's knowledge of the policies and practices—both current and planned—to protect the identified assets. The protection strategy outlines what is being done to protect the staff's important information assets. This part of the process answers the following question:

   - What are you currently doing to protect your assets?

   This activity uses the following inputs:

   - *Current knowledge of staff (I3.1)*—the knowledge of the staff concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:

     - catalog of organization practices—a standard compilation of known good organizational practices

     - catalog of technical practices—a standard compilation of known good technical practices

     - catalog of training practices—a standard compilation of known good training practices

   - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

   - *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

   This activity produces the following output:

   - *Current staff protection strategy (O3.4)*—the current or planned protection strategy implemented by the staff.

5. **Identify risk indicators**—elicits the staff's knowledge of known gaps in the current protection strategy. Risk indicators are typically organizational issues. Examples include not having an adequate security training and awareness program for the staff and not

having documented policies and procedures for protecting information assets. This part of the process answers the following question:

- What gaps in your current protection strategy are putting your assets at risk?

This activity uses the following inputs:

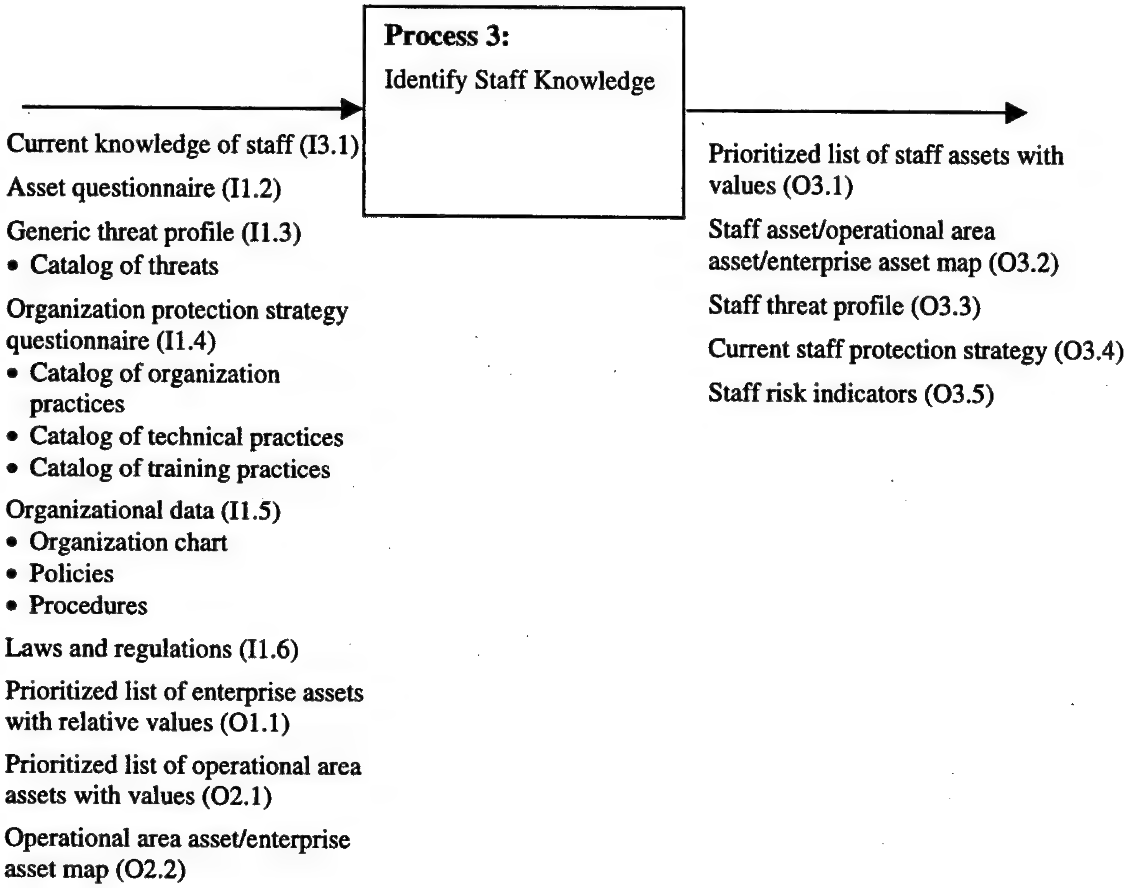
- *Current knowledge of staff (I3.1)*—the knowledge of the staff concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.
- *Organization protection strategy questionnaire (I1.4)*—an instrument designed to elicit information about the current protection strategy. This questionnaire is created by incorporating the following catalogs of information:
  - catalog of organization practices—a standard compilation of known good organizational practices
  - catalog of technical practices—a standard compilation of known good technical practices
  - catalog of training practices—a standard compilation of known good training practices
- *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.
- *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

This activity produces the following output:

- *Staff risk indicators (O3.5)*—concerns expressed by the staff indicating that there is a potential for assets to be at risk.

2.3.2 Diagram for Process 3: Identify Staff Knowledge

The following is the process diagram of Process 3. The diagram highlights the inputs and outputs to the process.



Process 3:
Identify Staff Knowledge

Current knowledge of staff (I3.1)

Asset questionnaire (I1.2)

Generic threat profile (I1.3)
- Catalog of threats

Organization protection strategy questionnaire (I1.4)
- Catalog of organization practices
- Catalog of technical practices
- Catalog of training practices

Organizational data (I1.5)
- Organization chart
- Policies
- Procedures

Laws and regulations (I1.6)

Prioritized list of enterprise assets with relative values (O1.1)

Prioritized list of operational area assets with values (O2.1)

Operational area asset/enterprise asset map (O2.2)

Prioritized list of staff assets with values (O3.1)

Staff asset/operational area asset/enterprise asset map (O3.2)

Staff threat profile (O3.3)

Current staff protection strategy (O3.4)

Staff risk indicators (O3.5)

Figure 6: OCTAVE Process 3, Identify Staff Knowledge

2.4 Process 4: Establish Security Requirements

OCTAVE's fourth process, Establish Security Requirements, builds upon the information gathered in the first three processes. Information from the individual perspectives is collected and combined where appropriate, and security requirements for the assets are determined. This provides enough information to form the basis for a protection strategy for the enterprise.

The goals of this process are to combine individual perspectives identified in the first three processes to create a composite picture of assets, threats, and risk indicators; to determine the enterprise-wide security requirements; and to create the foundation for the enterprise protection strategy. The following sections examine the activities and provide an input/output diagram for Process 4.

2.4.1 Activities

The inputs for this process are the data generated by the first three processes as well as the knowledge of the enterprise staff. The outputs are artifacts that capture the transformed information. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 4 are the following:

1. **Map assets identified in prior processes**—examines the relationships among the assets identified by personnel from different levels within the enterprise. This activity builds on the mapping performed in Processes 2 and 3 by incorporating additional perspectives. The result is a mapping of the relationships taking the different perspectives into account. Any items that cannot be mapped are also noted. The final part of this activity is the identification of the assets that are most important to the enterprise. This part of the process answers the following questions:

    - What is the composite view of the assets?
    - What are the relationships among the assets identified at different levels of the enterprise?
    - Which assets are most critical to the enterprise?

    This activity uses the following inputs:

    - *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

- *Prioritized list of enterprise assets with relative values (O1.1)*—a prioritized ordering of important assets and their relative values from the perspective of senior management.

- *Prioritized list of operational area assets with values (O2.1)*—a prioritized ordering of important assets and their relative values from the perspective of operational area management.

- *Prioritized list of staff assets with values (O3.1)*—a prioritized ordering of important assets and their relative values from the staff's perspective.

- *Staff asset/operational area asset/enterprise asset map (O3.2)*—documented relationships or mapping among staff assets, operational area assets, and enterprise assets.

This activity produces the following output:

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

2. **Combine threats identified in prior processes**—combines the threats identified by personnel from different levels within the enterprise. Threats indicate what or whom the assets are being protected from. This part of the process answers the following question:

   - What is the composite view of threats?

   This activity uses the following inputs:

   - *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Enterprise threat profile (O1.2)*—the threats to enterprise assets from the perspective of senior management.

   - *Operational area threat profile (O2.3)*—the threats to operational area assets from the perspective of operational area management.

   - *Staff threat profile (O3.3)*—the threats to staff assets from the staff's perspective.

   This activity produces the following output:

- *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

3. **Collect protection strategies**—collates the current protection strategies employed by the enterprise. The protection strategy outlines what is being done to protect the organization's important information assets. This part of the process answers the following question:

   - What is the complete set of current protection strategies identified by the different levels of the enterprise?

   This activity uses the following inputs:

   - *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

   - *Current enterprise protection strategy (O1.3)*—the enterprise's current or planned protection strategy from the perspective of senior management.

   - *Current operational area protection strategy (O2.4)*—the operational area's current or planned protection strategy from the perspective of operational area management.

   - *Current staff protection strategy (O3.4)*—the current or planned protection strategy implemented by the staff.

   This activity produces the following output:

   - *Current protection strategies (O4.3)*—the current or planned protection strategies identified by different levels within the enterprise.

4. **Collect risk indicators**—collates the risk indicators identified by personnel from different levels within the enterprise. Risk indicators are typically organizational issues. Examples include not having an adequate security training and awareness program for the staff and not having documented policies and procedures for protecting information assets. This part of the process answers the following question:

   - What is the complete set of risk indicators identified by the enterprise?

   This activity uses the following inputs:

- *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

- *Enterprise risk indicators (O1.4)*—concerns expressed by senior management indicating that there is a potential for assets to be at risk.

- *Operational area risk indicators (O2.5)*—concerns expressed by operational area management indicating that there is a potential for assets to be at risk.

- *Staff risk indicators (O3.5)*—concerns from the staff's perspective indicating that there is a potential for assets to be at risk.

This activity produces the following output:

- *Risk indicators (O4.4)*—concerns from different levels within the enterprise indicating that there is a potential for assets to be at risk.

5. **Establish security requirements**—identifies the requirements with respect to confidentiality, integrity, and availability of the identified assets. This part of the process answers the following questions for each asset:

- What are the requirements of the asset with respect to confidentiality?

- What are the requirements of the asset with respect to integrity?

- What are the requirements of the asset with respect to availability?

This activity uses the following input:

- *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

- *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

- *Current protection strategies (O4.3)*—the current or planned protection strategies identified by different levels within the enterprise.

- *Risk indicators (O4.4)*—concerns from different levels within the enterprise indicating that there is a potential for assets to be at risk.

This activity produces the following output:

- *Security requirements (O4.5)*—the requirements with respect to the confidentiality, integrity, and availability of the identified assets.

6. **Establish basis for protection strategy**—combines the outputs from the previous activities in Process 4 to produce a blueprint for the protection strategy. The blueprint outlines the following for each asset: threats, risk indicators, current protection strategies, and security requirements. The details of the protection strategy will be generated in Phase 3 of OCTAVE. This part of the process answers the following questions for each asset:

- What are the threats and risk indicators affecting the asset?

- What current protection strategies are in place for the asset?

- What are the security requirements for the asset?

This activity uses the following inputs:

- *Current knowledge of enterprise staff (I4.1)*—the knowledge of key enterprise staff members concerning important assets, threats to the assets, current protection strategies, and potential risk indicators.

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

- *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

- *Current protection strategies (O4.3)*—the current or planned protection strategies identified by different levels within the enterprise.

- *Risk indicators (O4.4)*—concerns from different levels within the enterprise indicating that there is a potential for assets to be at risk.

- *Security requirements (O4.5)*—the requirements with respect to the confidentiality, integrity, and availability of the identified assets.

This activity produces the following output:

- *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:
  - threats to the asset
  - risk indicators that might affect the asset
  - current strategies to protect the asset
  - security requirements for the asset

2.4.2 Diagram

The following is the process diagram of Process 4. The diagram highlights the inputs and outputs to the process.

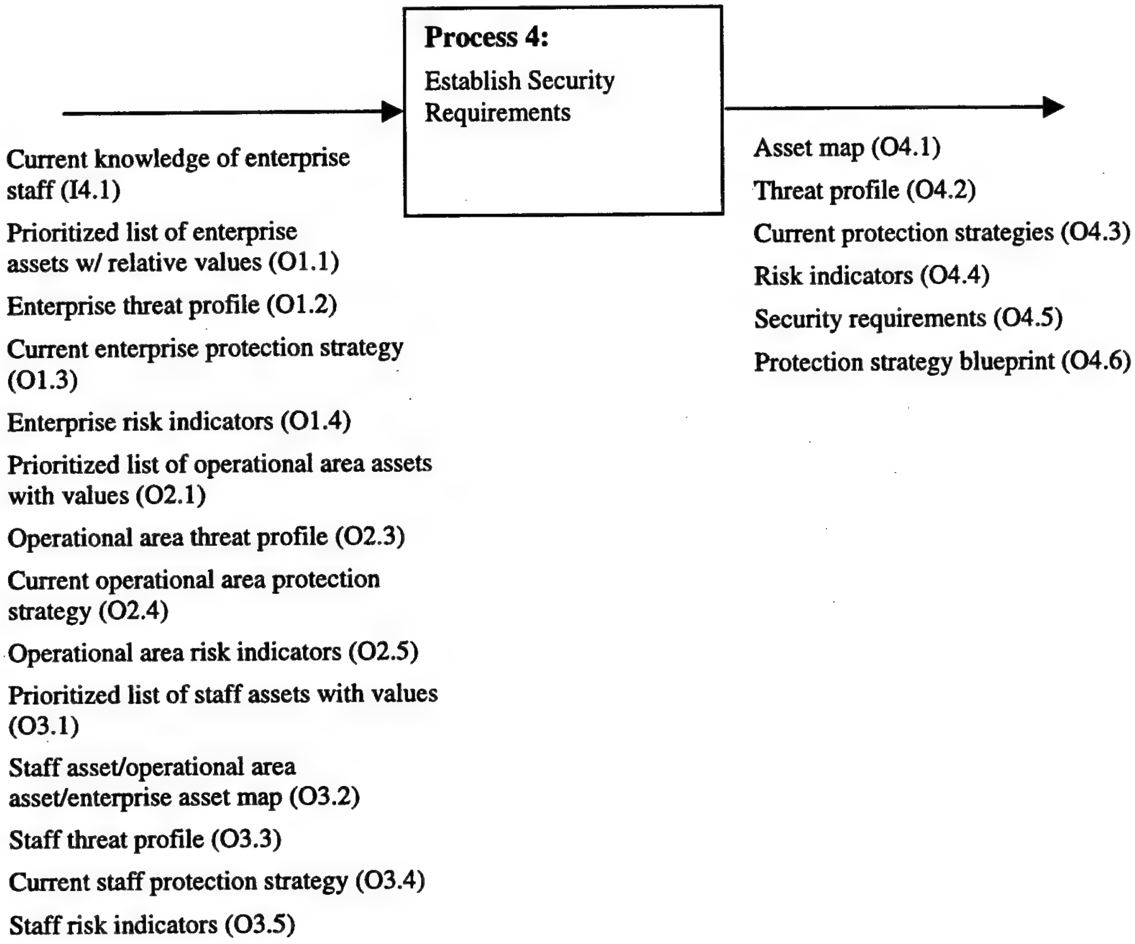

Process 4:
Establish Security Requirements
Current knowledge of enterprise staff (I4.1)
Prioritized list of enterprise assets w/ relative values (O1.1)
Enterprise threat profile (O1.2)
Current enterprise protection strategy (O1.3)
Enterprise risk indicators (O1.4)
Prioritized list of operational area assets with values (O2.1)
Operational area threat profile (O2.3)
Current operational area protection strategy (O2.4)
Operational area risk indicators (O2.5)
Prioritized list of staff assets with values (O3.1)
Staff asset/operational area asset/enterprise asset map (O3.2)
Staff threat profile (O3.3)
Current staff protection strategy (O3.4)
Staff risk indicators (O3.5)
Asset map (O4.1)
Threat profile (O4.2)
Current protection strategies (O4.3)
Risk indicators (O4.4)
Security requirements (O4.5)
Protection strategy blueprint (O4.6)

Figure 7: OCTAVE Process 4, Establish Security Requirements

3 Phase 2: Identify Infrastructure Vulnerabilities

Phase 2 of OCTAVE, Identify Infrastructure Vulnerabilities, has two processes. It builds on the information identified during Phase 1 by identifying the high-priority infrastructure components and the vulnerabilities that are exposing the enterprise's assets.

Phase 2 uses the asset and threat information from Phase 1 to identify the high-priority components of the information infrastructure (both the physical infrastructure and the computing infrastructure). It also evaluates the information infrastructure to identify vulnerabilities.

Standard catalogs of information about intrusion scenarios and vulnerabilities are used as a basis for evaluating the infrastructure. The ultimate goal of Phase 2 is to identify missing policies and practices as well as infrastructure vulnerabilities. The following two processes comprise Phase 2 of OCTAVE:

- Process 5, Map High-Priority Information Assets to Information Infrastructure. This process combines Phase 1 asset and threat information with staff knowledge about the information infrastructure to establish asset locations, access paths, and data flows. This leads to the identification of the high-priority infrastructure components.
- Process 6, Perform Infrastructure Vulnerability Evaluation. This process combines the knowledge about assets, threats, risk indicators, and security requirements determined in Phase 1 with staff knowledge about the information infrastructure and standard catalogs of intrusion scenarios and vulnerabilities to identify missing policies and practices as well as infrastructure vulnerabilities.

We will examine each of these processes in the following sections.

3.1 Process 5: Map High-Priority Information Assets to Information Infrastructure

OCTAVE's fifth process, Map High-Priority Information Assets to Information Infrastructure, defines the activity of taking the asset and threat information from Phase 1 and identifying the high-priority components of the information infrastructure. The information infrastructure refers to both the computing infrastructure as well as the physical infrastructure.

The goal of this process is to identify the most critical or high-priority components of the infrastructure so that they can be examined for vulnerabilities. The following sections describe the activities and provide an input/output diagram for Process 5.

3.1.1 Activities

The inputs for this process are threat and asset information from Phase 1; the knowledge of the project, information technology (IT), and facilities staffs; the physical layout of the information infrastructure; and artifacts required by the process (such as standard catalogs of information). The outputs are artifacts that capture the transformed information. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 5 are the following:

1. **Identify configuration of the information infrastructure**—examines documented artifacts and the knowledge of the staff concerning the information infrastructure. The documented artifacts used as inputs to this activity might not be current. The purpose of this activity is to produce updated documentation to reflect the state of the present computing and physical infrastructures. This part of the process answers the following questions:

   - What is the network topology?

   - What is the layout of the physical infrastructure?

   This activity uses the following inputs:

   - *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

   - *Current network topology diagrams (I5.2)*—existing diagrams and related documentation describing the layout of the enterprise's computing infrastructure.

   - *Current physical layout (I5.3)*—existing diagrams and related documentation describing the layout of the enterprise's physical infrastructure.

   This activity produces the following output:

   - *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

2. **Consolidate identified assets with identified infrastructure**—maps the important assets to the computing and physical infrastructures. This part of the process answers the following question:

   - Where are the important assets located in the infrastructure?

   This activity uses the following inputs:

   - *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

   - *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

   - *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

   This activity produces the following output:

   - *Asset locations in information infrastructure (O5.2)*—a mapping that show where the most important assets to the enterprise are located in the information infrastructure.

3. **Examine all access paths**—traces paths to the important assets via the computing and physical infrastructures. This part of the process answers the following questions:

   - Which assets can you access?

   - How can you get to those assets?

   This activity uses the following inputs:

- *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

- *Catalog of intrusion scenarios (I5.4)*—a standard compilation of known intrusion scenarios.

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

- *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *Asset locations in information infrastructure (O5.2)*—a mapping that show where the most important assets to the enterprise are located in the information infrastructure.

This activity produces the following output:

- *Asset access paths (O5.3)*—access paths to the important assets via the computing and physical infrastructures.

4. **Examine data flows**—traces data flows of the important assets via the computing and physical infrastructures. This part of the process answers the following question:

- Where in the infrastructure can assets move (either physically or via a network)?

This activity uses the following inputs:

- *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

- *Catalog of intrusion scenarios (I5.4)*—a standard compilation of known intrusion scenarios.

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

- *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *Asset locations in information infrastructure (O5.2)*—a mapping that show where the most important assets to the enterprise are located in the information infrastructure.

- *Asset access paths (O5.3)*—access paths to the important assets via the computing and physical infrastructures.

This activity produces the following output:

- *Asset data flows (O5.4)*—data flows of the important assets via the computing and physical infrastructures.

5. **Identify supporting/related assets**—identifies any assets that might support an important asset in some way. For example, operating system or database software might be needed to access important assets, making it a supporting asset. This part of the process answers the following question:

   - Are there any supporting or related assets (such as operating system or database software) that are critical to using the asset?

   This activity uses the following inputs:

   - *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

   - *Catalog of intrusion scenarios (I5.4)*—a standard compilation of known intrusion scenarios.

   - *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

   - *Threat profile (O4.2)*—the threats to organization's assets as identified by multiple levels of the organization.

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *Asset locations in information infrastructure (O5.2)*—a mapping that show where the most important assets to the enterprise are located in the information infrastructure.

- *Asset access paths (O5.3)*—access paths to the important assets via the computing and physical infrastructures.

- *Asset data flows (O5.4)*—data flows of the important assets via the computing and physical infrastructures.

This activity produces the following output:

- *Supporting/related assets (O5.5)*—assets that support or are related to an important asset.

6. **Determine high-priority components of the infrastructure**—identify the high-priority components of the infrastructure by analyzing the outputs from the previous activities in Process 5. These are identified by considering asset locations in the information infrastructure, asset access paths, asset data flows, and supporting/related assets. This part of the process answers the following question:

   - Which are the high-priority components of the infrastructure?

   This activity uses the following inputs:

   - *Current knowledge of project, IT, and facilities staffs (I5.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and the physical infrastructure.

   - *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

   - *Asset locations in information infrastructure (O5.2)*—a mapping that show where the most important assets to the enterprise are located in the information infrastructure.

   - *Asset access paths (O5.3)*—access paths to the important assets via the computing and physical infrastructures.

- *Asset data flows (O5.4)*—data flows of the important assets via the computing and physical infrastructures.

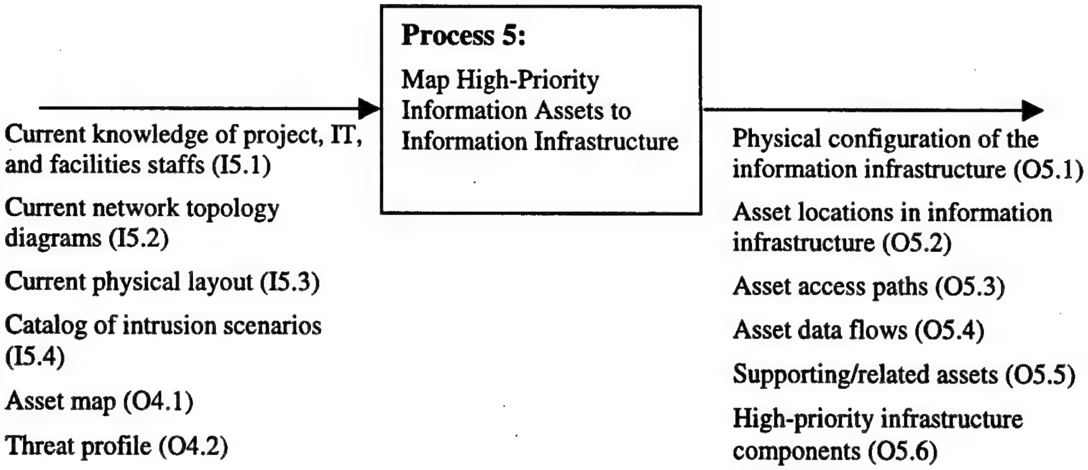
- *Supporting/related assets (O5.5)*—assets that support or are related to an important asset.

This activity produces the following output:

- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

3.1.2 Diagram

The following is the process diagram of Process 5. The diagram highlights the inputs and outputs to the process.



Process 5:

Map High-Priority Information Assets to Information Infrastructure

Current knowledge of project, IT, and facilities staffs (I5.1)

Current network topology diagrams (I5.2)

Current physical layout (I5.3)

Catalog of intrusion scenarios (I5.4)

Asset map (O4.1)

Threat profile (O4.2)

Physical configuration of the information infrastructure (O5.1)

Asset locations in information infrastructure (O5.2)

Asset access paths (O5.3)

Asset data flows (O5.4)

Supporting/related assets (O5.5)

High-priority infrastructure components (O5.6)

Figure 8: OCTAVE Process 5, Map High-Priority Information Assets to Information Infrastructure

3.2 Process 6: Perform Infrastructure Vulnerability Evaluation

OCTAVE's sixth process, Perform Infrastructure Vulnerability Evaluation, defines the activity of evaluating the vulnerability of the high-priority information infrastructure components identified in Process 5. The information infrastructure refers to both the computing infrastructure as well as the physical infrastructure.

The goal of this process is to identify the vulnerabilities present in the existing infrastructure and to identify missing policies or practices. The following sections examine the activities and provide an input/output diagram for Process 6.

3.2.1 Activities

The inputs for this process are the protection strategy blueprint from Phase 1; the knowledge of the project, information technology (IT), and facilities staffs; the physical layout of the information infrastructure; and artifacts required by the process (such as standard catalogs of information). The outputs are artifacts that capture the transformed information. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 6 are the following:

1. **Select intrusion scenarios**—identifies potential intrusion scenarios based on the characteristics of the enterprise. Characteristics include important assets, threats to the asset, risk indicators that might affect the asset, current strategies to protect the asset, security requirements for the asset, physical configuration of the information infrastructure, and high-priority infrastructure components. This part of the process answers the following question:

    - What intrusion scenarios could occur, considering the characteristics of the enterprise?

    This activity uses the following inputs:

    - *Current knowledge of project, IT, and facilities staffs (I6.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and physical infrastructure.

    - *Catalog of intrusion scenarios (I5.4)*—a standard compilation of known intrusion scenarios.

- *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:
    - threats to the asset
    - risk indicators that might affect the asset
    - current strategies to protect the asset
    - security requirements for the asset
- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.
- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

This activity produces the following output:

- *Filtered intrusion scenarios* (O6.1)—the potential intrusion scenarios based on the characteristics of the enterprise.

2. **Set scope of the infrastructure examination**—defines the extent of the infrastructure evaluation by considering existing policies and practices, missing policies and practices, and vulnerabilities for which the enterprise should be examined. This part of the process answers the following questions:

    - What is the scope of the infrastructure evaluation?
    - Which policies and practices exist in the enterprise?
    - Which policies and practices are missing?
    - For which vulnerabilities should the enterprise be examined?

    This activity uses the following inputs:

    - *Current knowledge of project, IT, and facilities staffs (I6.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and physical infrastructure.
    - *Catalog of vulnerabilities (I6.2)*—a standard compilation of known vulnerabilities.

- *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

- *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

- *Filtered intrusion scenarios* (O6.1)—the potential intrusion scenarios based on the characteristics of the enterprise.

This activity produces the following outputs:

- *Existing policies and practices (O6.2)*—policies and practices that are identified by the organization and are also evident in the organization.

- *Missing policies and practices (O6.3)*—policies and practices that are identified by the organization as required but are not in place.

- *Infrastructure components to examine (O6.4)*—the infrastructure components selected to be reviewed as part of the infrastructure examination.

- *Potential vulnerabilities (O6.5)*—the vulnerabilities that will be tested for based on the infrastructure components to be examined.

3. **Examine infrastructure**—performs the infrastructure evaluation to identify which vulnerabilities are present. This part of the process answers the following question:

   - Which vulnerabilities are present?

   This activity uses the following inputs:

   - *Current knowledge of project, IT, and facilities staffs (I6.1)*—the knowledge of the staff concerning important assets, threats to the assets, network topology, and physical infrastructure.

   - *Catalog of vulnerabilities (I6.2)*—a standard compilation of known vulnerabilities.

- *Technology information (I6.3)*—any documentation, software tools, or artifacts used by the enterprise to design and manage their information infrastructure. Examples include architecture documents, router tables, logs, and audit data.

- *Software tools (I6.4)*—tools to assist with or automate the infrastructure evaluation process.

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

- *Infrastructure components to examine (O6.4)*—the infrastructure components selected to be reviewed as part of the infrastructure examination.

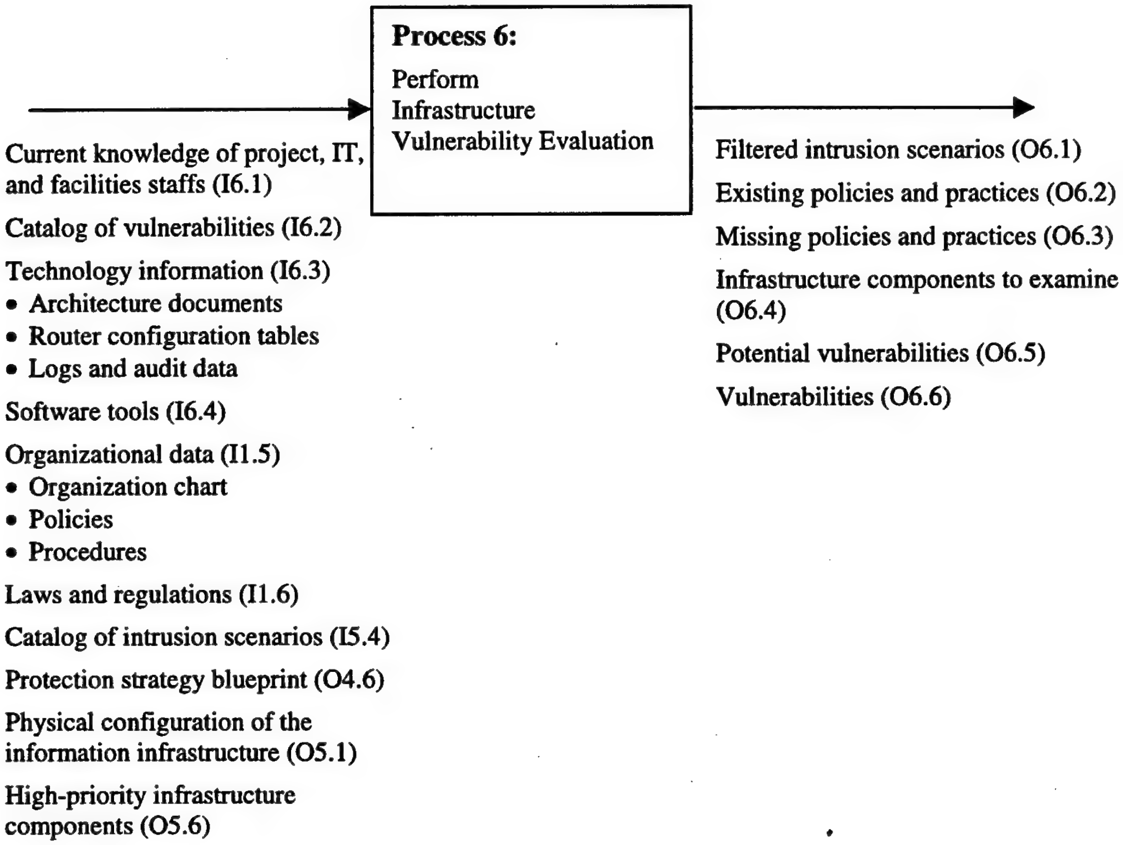
- *Potential vulnerabilities (O6.5)*—the vulnerabilities that will be tested for based on the infrastructure components to be examined.

This activity produces the following output:

- *Vulnerabilities (O6.6)*—the vulnerabilities that are found to be present in the enterprise, based on the infrastructure examination.

3.2.2 Diagram

The following is the process diagram of Process 6. The diagram highlights the inputs and outputs to the process.



Process 6:

Perform Infrastructure Vulnerability Evaluation

Current knowledge of project, IT, and facilities staffs (I6.1)

Catalog of vulnerabilities (I6.2)

Technology information (I6.3)
- Architecture documents
- Router configuration tables
- Logs and audit data

Software tools (I6.4)

Organizational data (I1.5)
- Organization chart
- Policies
- Procedures

Laws and regulations (I1.6)

Catalog of intrusion scenarios (I5.4)

Protection strategy blueprint (O4.6)

Physical configuration of the information infrastructure (O5.1)

High-priority infrastructure components (O5.6)

Filtered intrusion scenarios (O6.1)

Existing policies and practices (O6.2)

Missing policies and practices (O6.3)

Infrastructure components to examine (O6.4)

Potential vulnerabilities (O6.5)

Vulnerabilities (O6.6)

Figure 9: OCTAVE Process 6, Perform Infrastructure Vulnerability Evaluation

4 Phase 3: Determine Security Risk Management Strategy

Phase 3 of OCTAVE, Determine Security Risk Management Strategy, has two processes. It analyzes asset, threat, and vulnerability information in the context of intrusion scenarios to identify and prioritize the risks to the enterprise. In addition, a protection strategy is developed and implemented in the enterprise.

The ultimate goal of Phase 3 is to identify risks to the enterprise and develop a protection strategy to mitigate the highest priority risks. The following two processes comprise Phase 3 of OCTAVE:

- Process 7, Conduct Multi-Dimensional Risk Analysis. This process analyzes the asset, threat, and vulnerability information identified in Phases 1 and 2 using intrusion scenarios to produce a set of risks to the enterprise. The risk attributes of impact and probability are estimated and then used to prioritize the risks.

- Process 8, Develop Protection Strategy. This process develops the protection strategy by identifying candidate mitigation strategies and then selecting the appropriate ones based on factors such as cost and available resources. This process also develops a comprehensive security risk management plan for implementing the protection strategy and managing risks on a continual basis.

We will examine each of these processes in the following sections.

4.1 Process 7: Conduct Multi-Dimensional Risk Analysis

OCTAVE's seventh process, Conduct Multi-Dimensional Risk Analysis, is the activity of identifying and prioritizing risks to the enterprise. Risks are defined based on the knowledge of the staff as well as an understanding of validated intrusion scenarios, exposed assets, impacts of exposed assets, threats to the exposed assets, and threat probabilities.

The goal of this process is to generate a prioritized list of risks based on impact and probability. The following sections examine the activities and provide an input/output diagram for Process 7.

4.1.1 Activities

The inputs for this process include the knowledge of the enterprise staff, asset and threat information from Phase 1, and vulnerability and intrusion scenario information from Phase 2. The outputs are artifacts that capture the transformed information. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 7 are the following:

1. **Determine points of vulnerability in potential intrusion scenarios**—examines potential intrusion scenarios for points of vulnerability, based on the identified vulnerabilities. Identifies which intrusion scenarios are possible based on the vulnerabilities. This part of the process answers the following questions for each potential intrusion scenario:

   - Which of the identified vulnerabilities can be exploited in this scenario?

   - Are any of the enterprise assets exposed by this scenario?

   This activity uses the following inputs:

   - *Current knowledge of enterprise staff (I7.1)*—the knowledge of the staff concerning important assets, threats to the assets, vulnerabilities, and intrusion scenarios.

   - *Risk indicators (O4.4)*—concerns from different levels within the enterprise indicating that there is a potential for assets to be at risk.

   - *Filtered intrusion scenarios* (O6.1)—the potential intrusion scenarios based on the characteristics of the enterprise.

- *Missing policies and practices (O6.3)*—policies and practices that are identified by the organization as required but are not in place.

- *Vulnerabilities (O6.6)*—the vulnerabilities that are found to be present in the enterprise, based on the infrastructure examination.

This activity produces the following output:

- *Validated intrusion scenarios (O7.1)*—the intrusion scenarios containing points of vulnerability and exposing important assets.

2. **Examine assets exposed by the validated intrusion scenarios**—identifies assets exposed by the validated intrusion scenarios and determines the impact of exposed assets to the enterprise. This part of the process answers the following questions for each validated intrusion scenario:

- Which assets does this scenario expose?

- What is the impact the asset is compromised?

This activity uses the following inputs:

- *Current knowledge of enterprise staff (I7.1)*—the knowledge of the staff concerning important assets, threats to the assets, vulnerabilities, and intrusion scenarios.

- *Asset map (O4.1)*—a mapping that shows the relationships among the assets identified by the three levels of the organization. The asset map also identifies those assets that are most important to the enterprise.

- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

- *Validated intrusion scenarios (O7.1)*—the intrusion scenarios containing points of vulnerability and exposing important assets.

This activity produces the following outputs:

- *Exposed assets (O7.2)*—assets that are exposed to points of vulnerability from the validated intrusion scenarios.

- *Impact of exposed assets (O7.3)*—the impact to the enterprise if assets are compromised. This is derived from the value of the assets identified in Phase 1 and included in the asset map.

3. **Examine threats to the exposed assets**—assigns probabilities for each threat based on the exposed assets and the possible intrusion scenarios. The highest threat probability for each exposed asset will be considered in later activities. This part of the process answers the following questions for each possible intrusion scenario:

   - What is the likelihood that a threat will access the exposed assets?

   - Which threat has the greatest likelihood of accessing the exposed assets?

   This activity uses the following inputs:

   - *Current knowledge of enterprise staff (I7.1)*—the knowledge of the staff concerning important assets, threats to the assets, vulnerabilities, and intrusion scenarios.

   - *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:

     - threats to the asset

     - risk indicators that might affect the asset

     - current strategies to protect the asset

     - security requirements for the asset

   - *Validated intrusion scenarios (O7.1)*—the intrusion scenarios containing points of vulnerability and exposing important assets.

   - *Exposed assets (O7.2)*—assets that are exposed to points of vulnerability from the validated intrusion scenarios.

   This activity produces the following output:

   - *Threat probability (O7.4)*—the likelihood that a threat will compromise an exposed asset.

4. **Construct a statement of risk**—defines statements of risk based on the knowledge of the staff along with an understanding of validated intrusion scenarios, exposed assets, impacts of exposed assets, threats to the exposed assets, and threat probabilities. This part of the process answers the following questions for each possible intrusion scenario:

   - What are the risks?

- How can the risks be communicated to others?

This activity uses the following inputs:

- *Current knowledge of enterprise staff (I7.1)*—the knowledge of the staff concerning important assets, threats to the assets, vulnerabilities, and intrusion scenarios.
- *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:
  - threats to the asset
  - risk indicators that might affect the asset
  - current strategies to protect the asset
  - security requirements for the asset
- *Validated intrusion scenarios (O7.1)*—the intrusion scenarios containing points of vulnerability and exposing important assets.
- *Exposed assets (O7.2)*—assets that are exposed by points of vulnerability on the intrusion scenarios.
- *Impact of exposed assets (O7.3)*—the impact to the enterprise if assets are compromised. This is derived from the value of the assets identified in Phase 1 and included in the asset map.
- *Threat probability (O7.4)*—the likelihood that a threat will compromise an exposed asset.

This activity produces the following output:

- *Risks (O7.5)*—statements of risks based on threats to exposed assets. An impact value and a threat probability (that is, the risk attributes) are associated with each risk statement.

5. **Determine priority risks to the enterprise**—prioritizes the risks based on their impacts and probabilities. This part of the process answers the following question:

   - What are the greatest risks to the enterprise based on impact and probability?

   This activity uses the following inputs:

- *Current knowledge of enterprise staff (I7.1)*—the knowledge of the staff concerning important assets, threats to the assets, vulnerabilities, and intrusion scenarios.

- *Impact of exposed assets (O7.3)*—the impact to the enterprise if assets are compromised. This is derived from the value of the assets identified in Phase 1 and included in the asset map.

- *Threat probability (O7.4)*—the likelihood that a threat will compromise an exposed asset.

- *Risks (O7.5)*—statements of risks based on threats to exposed assets. An impact value and a threat probability (that is, the risk attributes) are associated with each risk statement.

This activity produces the following output:

- *Prioritized list of risks (O7.6)*—a priority ordering of the risks based on their impacts and probabilities.

4.1.2 Diagram

The following is the process diagram of Process 7. The diagram highlights the inputs and outputs to the process.

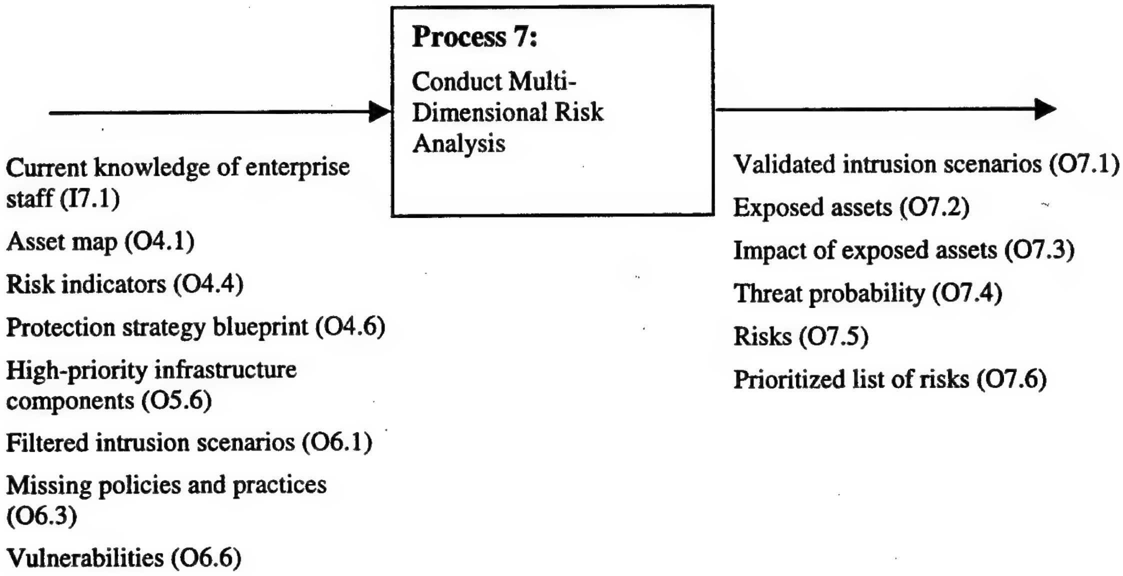

Process 7:
Conduct Multi-Dimensional Risk Analysis
Current knowledge of enterprise staff (I7.1)
Asset map (O4.1)
Risk indicators (O4.4)
Protection strategy blueprint (O4.6)
High-priority infrastructure components (O5.6)
Filtered intrusion scenarios (O6.1)
Missing policies and practices (O6.3)
Vulnerabilities (O6.6)
Validated intrusion scenarios (O7.1)
Exposed assets (O7.2)
Impact of exposed assets (O7.3)
Threat probability (O7.4)
Risks (O7.5)
Prioritized list of risks (O7.6)

Figure 10: OCTAVE Process 7, Conduct Multi-Dimensional Risk Analysis

4.2 Process 8: Develop Protection Strategy

OCTAVE's eighth process, Develop Protection Strategy, defines the activities of developing and implementing a strategy to protect the enterprise by reducing its information security risk.

The goal of this process is to produce a protection strategy for reducing risk and a risk management plan for managing risk on a continual basis.

4.2.1 Activities

The inputs for this process include the knowledge of enterprise management, project, and technical staffs; information about existing and missing policies and practices; vulnerabilities; laws and regulations; risks; and available funding and staff. The outputs are artifacts that capture the transformed information. Each input and output is tagged with an identification number to allow data to be traced among the processes of OCTAVE.

The activities for Process 8 are the following:

1. **Identify candidate mitigation approaches**—develops candidate approaches for mitigating the highest-priority risks by considering existing and missing policies and practices, threats, assets, vulnerabilities and available technology. This part of the process answers the following question:

    - What are potential approaches for mitigating the highest-priority risks?

    This activity uses the following inputs:

    - *Current knowledge of enterprise management, project, and technical staffs (I8.1)*—the knowledge of the management, project, and technical staffs concerning risks, mitigation approaches, and protection strategies.

    - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.

    - *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.

    - *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:

        - threats to the asset

        - risk indicators that might affect the asset

- current strategies to protect the asset
- security requirements for the asset

- *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.
- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.
- *Existing policies and practices (O6.2)*—policies and practices that are identified by the organization and are also evident in the organization.
- *Missing policies and practices (O6.3)*—policies and practices that are identified by the organization as required but are not in place.
- *Vulnerabilities (O6.6)*—the vulnerabilities that are found to be present in the enterprise, based on the infrastructure examination.
- *Exposed assets (O7.2)*—assets that are exposed by points of vulnerability on the intrusion scenarios.
- *Impact of exposed assets (O7.3)*—the impact to the enterprise if assets are compromised. This is derived from the value of the assets identified in Phase 1 and included in the asset map.
- *Threat probability (O7.4)*—the likelihood that a threat will compromise an exposed asset.
- *Risks (O7.5)*—statements of risks based on threats to exposed assets. An impact value and a threat probability (that is, the risk attributes) are associated with each risk statement.
- *Prioritized list of risks (O7.6)*—a priority ordering of the risks based on their impacts and probabilities.

This activity produces the following output:

- *Candidate mitigation approaches (O8.1)*—candidate approaches for mitigating the highest-priority risks.

2. **Develop protection strategy**—selects mitigation approaches to improve the security of the enterprise by considering the following: candidate mitigation approaches, impact on assets, the number of assets at risk, the cost of solutions, and resources available. This part of the process answers the following questions:

   - Which mitigation approaches will be included in your protection strategy?
   - How much money and staff do you have available?
   - How many assets are at risk?
   - What impact will your protection strategy have on your exposed assets?

   This activity uses the following inputs:

   - *Current knowledge of enterprise management, project, and technical staffs (I8.1)*—the knowledge of the management, project, and technical staffs concerning risks, mitigation approaches, and protection strategies.
   - *Available funding (I8.2)*—resources available to implement the protection strategy.
   - *Available staff (I8.3)*—staff available to implement the protection strategy.
   - *Organizational data (I1.5)*—documented organizational data, such as organization charts, policies, and procedures.
   - *Laws and regulations (I1.6)*—laws and regulations with which the enterprise must comply.
   - *Protection strategy blueprint (O4.6)*—a document that outlines the following information for each asset:
     - threats to the asset
     - risk indicators that might affect the asset
     - current strategies to protect the asset
     - security requirements for the asset
   - *Physical configuration of the information infrastructure (O5.1)*—diagrams and related documentation describing the layout of the enterprise's computing and physical infrastructures.

- *High-priority infrastructure components (O5.6)*—the components of the infrastructure that affect the important assets.

- *Existing policies and practices (O6.2)*—policies and practices that are identified by the organization and are also evident in the organization.

- *Missing policies and practices (O6.3)*—policies and practices that are identified by the organization as required but are not in place.

- *Vulnerabilities (O6.6)*—the vulnerabilities that are found to be present in the enterprise, based on the infrastructure examination.

- *Exposed assets (O7.2)*—assets that are exposed by points of vulnerability on the intrusion scenarios.

- *Impact of exposed assets (O7.3)*—the impact to the enterprise if assets are compromised. This is derived from the value of the assets identified in Phase 1 and included in the asset map.

- *Threat probability (O7.4)*—the likelihood that a threat will compromise an exposed asset.

- *Risks (O7.5)*—statements of risks based on threats to exposed assets. An impact value and a threat probability (that is, the risk attributes) are associated with each risk statement.

- *Prioritized list of risks (O7.6)*—a priority ordering of the risks based on their impacts and probabilities.

- *Candidate mitigation approaches (O8.1)*—candidate approaches for mitigating the highest-priority risks.

This activity produces the following output:

- *Protection strategy (O8.2)*—selected mitigation approaches that improve the security of the enterprise by reducing risk.

3. **Develop a comprehensive plan to manage security risks**—develops a comprehensive security risk management plan by considering how to implement the protection strategy and manage risks on a continual basis. This part of the process answers the following questions:

   - What is your plan for implementing your protection strategy?

- How do you plan to manage your security risks on a continual basis?
- What indicators do you plan to monitor for indications of new risk?
- When do plan to perform your next OCTAVE evaluation?

This activity uses the following inputs:

- *Current knowledge of enterprise management, project, and technical staffs (I8.1)*—the knowledge of the management, project, and technical staffs concerning risks, mitigation approaches, and protection strategies.
- *Available funding (I8.2)*—Resources available to implement the protection strategy.
- *Available staff (I8.3)*—Staff available to implement the protection strategy.
- *Prioritized list of risks (O7.6)*—a priority ordering of the risks based on their impacts and probabilities.
- *Protection strategy (O8.2)*—selected mitigation approaches that improve the security of the enterprise by reducing risk.

This activity produces the following output:

- *Security risk management plan (O8.3)*—a comprehensive plan that outlines how to implement the protection strategy and manage risks on a continual basis.

4. **Implement selected protection strategy**—implements and monitors the protection strategy for effectiveness. This part of the process answers the following question:

   - How will you measure the effectiveness of your protection strategy?

   This activity uses the following inputs:

   - *Current knowledge of enterprise management, project, and technical staffs (I8.1)*—the knowledge of the management, project, and technical staffs concerning risks, mitigation approaches, and protection strategies.
   - *Available funding (I8.2)*—resources available to implement the protection strategy.
   - *Available staff (I8.3)*—staff available to implement the protection strategy.

- *Prioritized list of risks (O7.6)*—a priority ordering of the risks based on their impacts and probabilities.

- *Protection strategy (O8.2)*—selected mitigation approaches that improve the security of the enterprise by reducing risk.

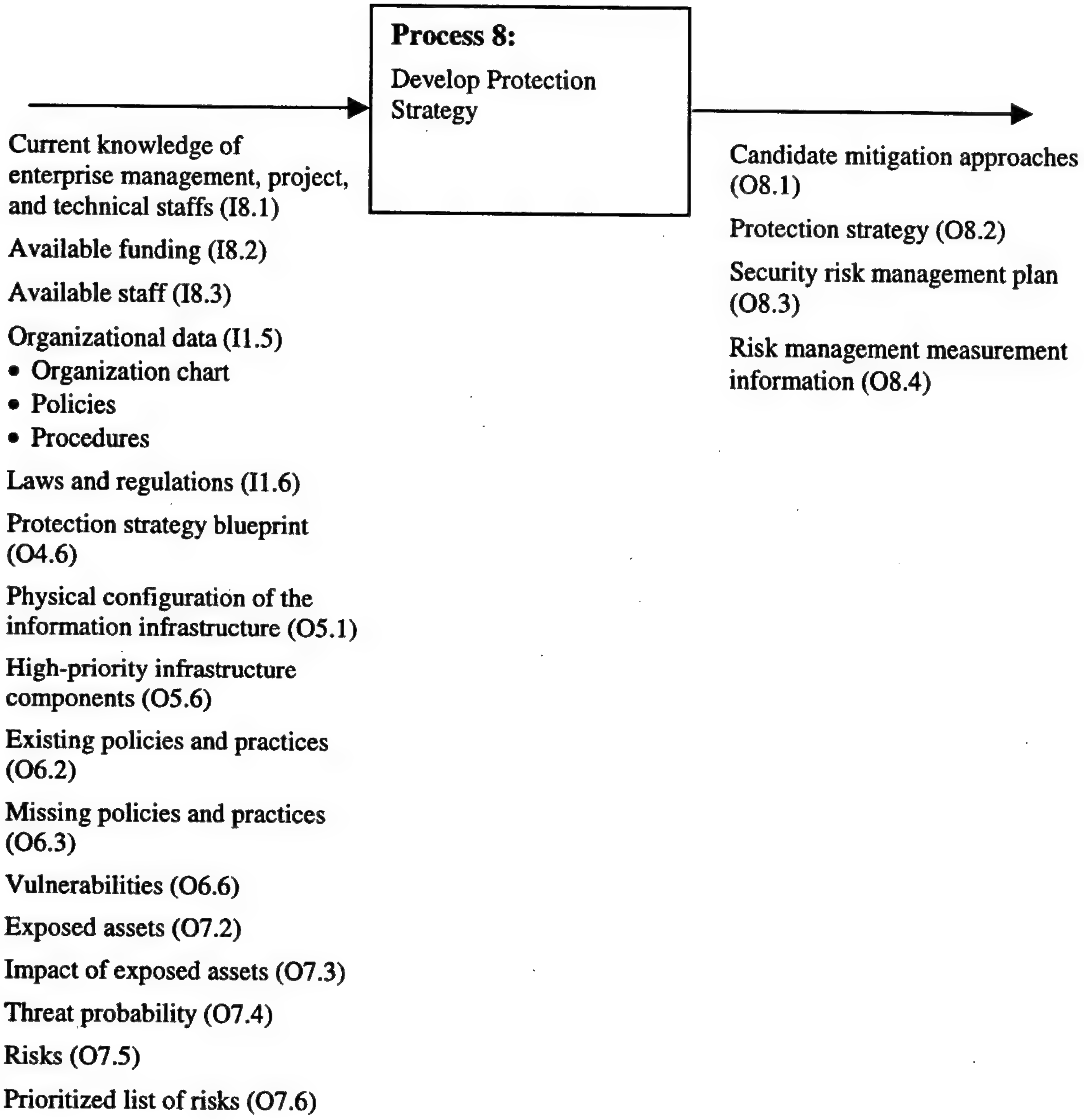
- *Security risk management plan (O8.3)*—a comprehensive plan that outlines how to implement the protection strategy and manage risks on a continual basis.

This activity produces the following output:

- *Risk management measurement information (O8.4)*—measurement information about the effectiveness of the protection strategy.

4.2.2 Diagram

The following is the process diagram of Process 8. The diagram highlights the inputs and outputs to the process.



Process 8:

Develop Protection Strategy

Current knowledge of enterprise management, project, and technical staffs (I8.1)

Available funding (I8.2)

Available staff (I8.3)

Organizational data (I1.5)

- Organization chart
- Policies
- Procedures

Laws and regulations (I1.6)

Protection strategy blueprint (O4.6)

Physical configuration of the information infrastructure (O5.1)

High-priority infrastructure components (O5.6)

Existing policies and practices (O6.2)

Missing policies and practices (O6.3)

Vulnerabilities (O6.6)

Exposed assets (O7.2)

Impact of exposed assets (O7.3)

Threat probability (O7.4)

Risks (O7.5)

Prioritized list of risks (O7.6)

Candidate mitigation approaches (O8.1)

Protection strategy (O8.2)

Security risk management plan (O8.3)

Risk management measurement information (O8.4)

Figure 11: OCTAVE Process 8, Develop Protection Strategy

5 Summary

OCTAVE is a framework for identifying and managing information security risks. It is designed to be a self-directed activity for organizations.

The framework requires the use of standard catalogs of information, which are known to the security community, to form a basis upon which to evaluate an organization. This leads to the identification of information assets and their values, threats to those assets, and infrastructure vulnerabilities exposing the assets to the threats. By analyzing the asset, threat, and vulnerability information in the context of intrusion scenarios, an organization can begin to understand what information is at risk. With this understanding, it can create and implement a protection strategy designed to reduce the overall risk exposure of its information assets.

OCTAVE consists of three phases and eight processes. Phase 1 has four processes, Phase 2 has two processes, and Phase 3 has two processes.

Phase 1 of OCTAVE, "Build Enterprise-Wide Security Requirements," examines the enterprise by eliciting information from people working in multiple levels of the enterprise. Integrating unique perspectives and knowledge from multiple organizational levels helps to build an enterprise-wide view of assets, threats, protection strategies, and risk indicators. Phase 1 also derives the security requirements of the enterprise, based on the need for confidentiality, integrity, and/or availability of the key information assets.

Phase 2 of OCTAVE, "Identify Infrastructure Vulnerabilities," builds on the information identified during Phase 1. It uses the asset and threat information from Phase 1 to identify the high-priority components of the information infrastructure. Phase 2 also evaluates the information infrastructure to identify infrastructure vulnerabilities that are exposing the enterprise's assets as well as missing policies and practices.

Phase 3, "Determine Security Risk Management Strategy," analyzes asset, threat, and vulnerability information in the context of intrusion scenarios to identify and prioritize the information security risks to the organization. In addition, it develops and implements a protection strategy in the organization to reduce the risk to the enterprise. Finally, Phase 3 creates a comprehensive risk management plan for implementing the protection strategy and managing risks on a continual basis.

5.1 OCTAVE Goals and Processes

The following list summarizes the goals and processes of the three OCTAVE phases.

Phase 1: Build Enterprise-Wide Security Requirements

Goal: Establish the security requirements of the enterprise.

Processes:

- **Process 1, Identify Enterprise Knowledge.** This process identifies what senior managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.

- **Process 2, Identify Operational Area Knowledge.** This process identifies what operational area managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.

- **Process 3, Identify Staff Knowledge.** This process identifies what staff-level personnel perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise

- **Process 4, Establish Security Requirements.** This process integrates the individual perspectives identified in the first three processes to produce an enterprise view of the assets, threats, protection strategies, and risk indicators. In addition, the security requirements of the enterprise are identified.

Phase 2: Identify Infrastructure Vulnerabilities

Goal: Identify infrastructure vulnerabilities and missing policies and practices.

Processes:

- **Process 5, Map High-Priority Information Assets to Information Infrastructure.** This process combines Phase 1 asset and threat information with staff knowledge about the information infrastructure to establish asset locations, access paths, and data flows. This leads to the identification of the high-priority infrastructure components.

- **Process 6, Perform Infrastructure Vulnerability Evaluation.** This process combines knowledge about assets, threats, risk indicators, and security requirements identified in Phase 1 with staff knowledge about the information infrastructure and standard catalogs of intrusion scenarios and vulnerabilities. This leads to the identification of missing policies and practices as well as infrastructure vulnerabilities.

Phase 3: Determine Security Risk Management Strategy

Goal: Identify risks and develop a protection strategy to reduce the highest priority risks to the enterprise.

Processes:

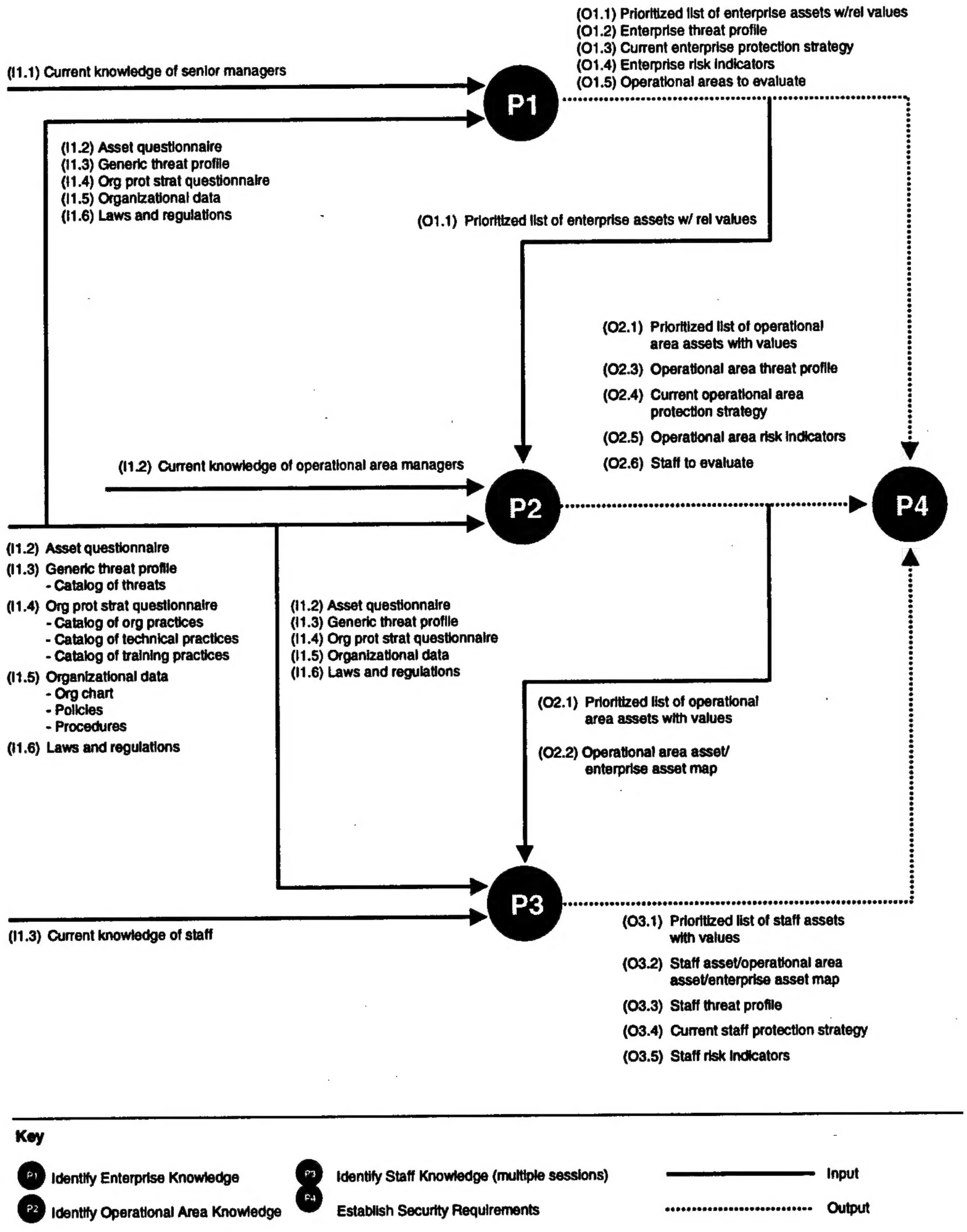
- **Process 7, Conduct Multi-Dimensional Risk Analysis**. This process analyzes the asset, threat, and vulnerability information identified in Phases 1 and 2 using intrusion scenarios to produce a set of risks to the enterprise. The risk attributes of impact and probability are estimated and then used to prioritize the risks.

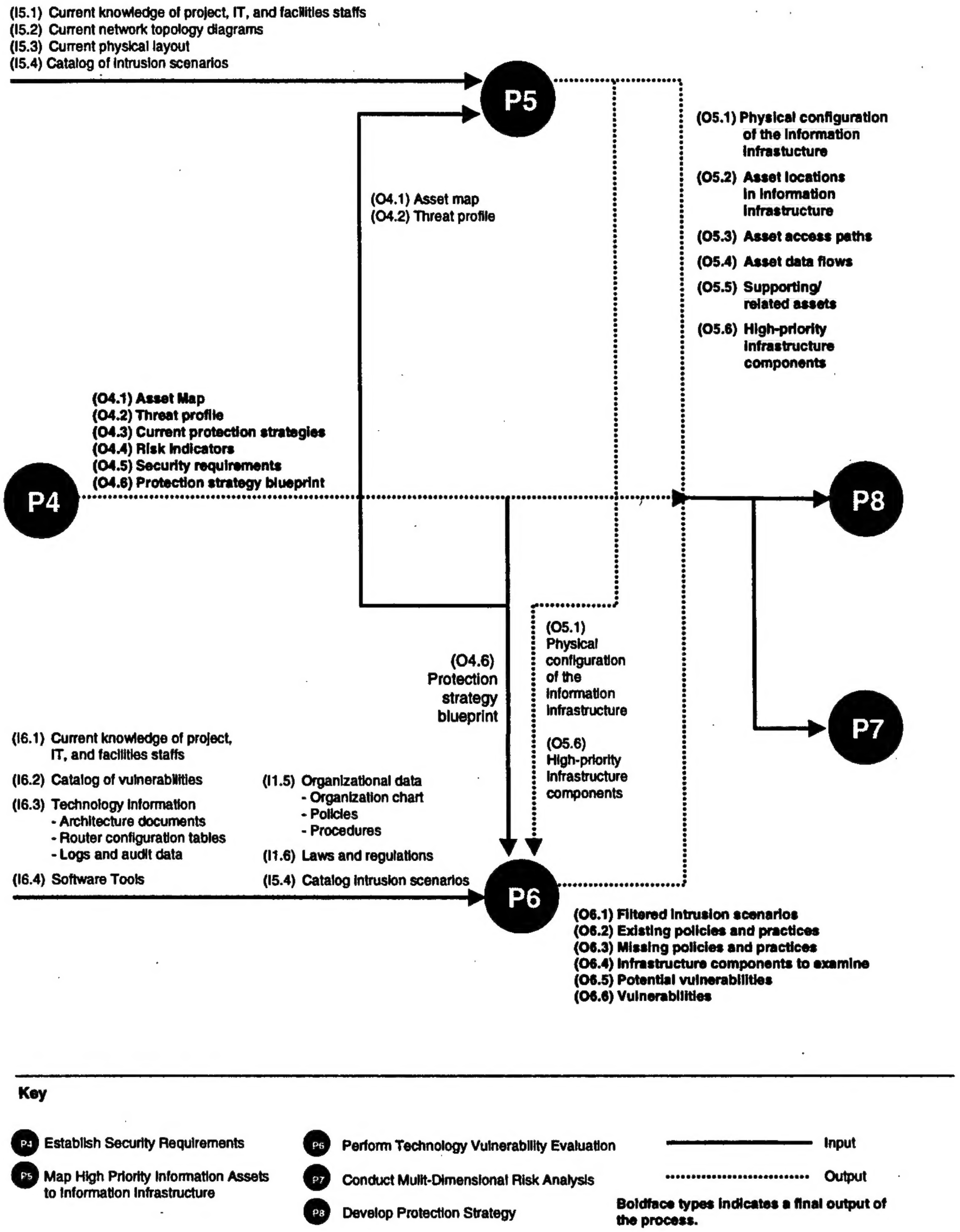
- **Process 8, Develop Protection Strategy**. This process develops the protection strategy by identifying candidate mitigation strategies and then selecting the appropriate ones based on factors such as cost and available resources. This process also develops a comprehensive security risk management plan for implementing the protection strategy and managing risks on a continual basis.

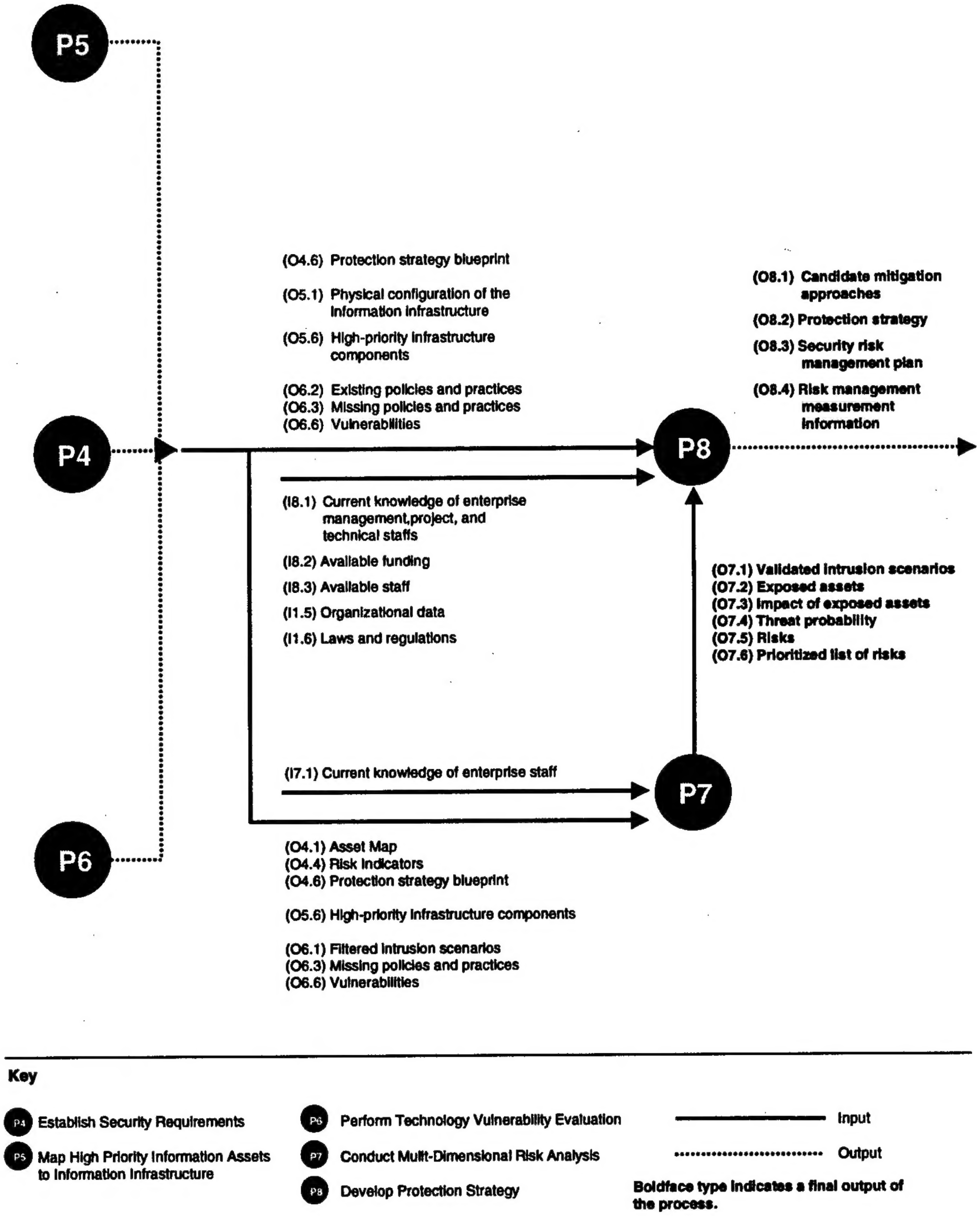
5.2 Future Plans

One of the purposes of issuing this report on the OCTAVE framework is to initiate a discussion among the members of the community concerning what comprises a comprehensive information security risk assessment. In addition, the Software Engineering Institute plans to develop a self-directed method consistent with the framework. We will pilot-test the method upon completion of development. The lessons that are learned from delivering the method and the comments from the community will be used to modify the framework and method as appropriate.

6 Appendix: OCTAVE Flowchart


(O1.1) Prioritized list of enterprise assets w/rel values
(O1.2) Enterprise threat profile
(O1.3) Current enterprise protection strategy
(O1.4) Enterprise risk indicators
(O1.5) Operational areas to evaluate
(I1.1) Current knowledge of senior managers
P1
(I1.2) Asset questionnaire
(I1.3) Generic threat profile
(I1.4) Org prot strat questionnaire
(I1.5) Organizational data
(I1.6) Laws and regulations
(O1.1) Prioritized list of enterprise assets w/ rel values
(O2.1) Prioritized list of operational area assets with values
(O2.3) Operational area threat profile
(O2.4) Current operational area protection strategy
(O2.5) Operational area risk indicators
(O2.6) Staff to evaluate
(I1.2) Current knowledge of operational area managers
P2
P4
(I1.2) Asset questionnaire
(I1.3) Generic threat profile
- Catalog of threats
(I1.4) Org prot strat questionnaire
- Catalog of org practices
- Catalog of technical practices
- Catalog of training practices
(I1.5) Organizational data
- Org chart
- Policies
- Procedures
(I1.6) Laws and regulations
(I1.2) Asset questionnaire
(I1.3) Generic threat profile
(I1.4) Org prot strat questionnaire
(I1.5) Organizational data
(I1.6) Laws and regulations
(O2.1) Prioritized list of operational area assets with values
(O2.2) Operational area asset/ enterprise asset map
P3
(I1.3) Current knowledge of staff
(O3.1) Prioritized list of staff assets with values
(O3.2) Staff asset/operational area asset/enterprise asset map
(O3.3) Staff threat profile
(O3.4) Current staff protection strategy
(O3.5) Staff risk indicators
Key
P1 Identify Enterprise Knowledge
P2 Identify Operational Area Knowledge
P3 Identify Staff Knowledge (multiple sessions)
P4 Establish Security Requirements
Input
Output


(I5.1) Current knowledge of project, IT, and facilities staffs
(I5.2) Current network topology diagrams
(I5.3) Current physical layout
(I5.4) Catalog of intrusion scenarios
P5
(O4.1) Asset map
(O4.2) Threat profile
(O5.1) Physical configuration of the information infrastucture
(O5.2) Asset locations in information infrastructure
(O5.3) Asset access paths
(O5.4) Asset data flows
(O5.5) Supporting/ related assets
(O5.6) High-priority infrastructure components
(O4.1) Asset Map
(O4.2) Threat profile
(O4.3) Current protection strategies
(O4.4) Risk indicators
(O4.5) Security requirements
(O4.6) Protection strategy blueprint
P4
P8
(O4.6) Protection strategy blueprint
(O5.1) Physical configuration of the information infrastructure
(O5.6) High-priority infrastructure components
P7
(I6.1) Current knowledge of project, IT, and facilities staffs
(I6.2) Catalog of vulnerabilities
(I6.3) Technology information
- Architecture documents
- Router configuration tables
- Logs and audit data
(I6.4) Software Tools
(I1.5) Organizational data
- Organization chart
- Policies
- Procedures
(I1.6) Laws and regulations
(I5.4) Catalog intrusion scenarios
P6
(O6.1) Filtered intrusion scenarios
(O6.2) Existing policies and practices
(O6.3) Missing policies and practices
(O6.4) Infrastructure components to examine
(O6.5) Potential vulnerabilities
(O6.6) Vulnerabilities
Key
P4 Establish Security Requirements
P5 Map High Priority Information Assets to Information Infrastructure
P6 Perform Technology Vulnerability Evaluation
P7 Conduct Mulit-Dimensional Risk Analysis
P8 Develop Protection Strategy
Input
Output
Boldface types indicates a final output of the process.


P5
P4
P6
P8
P7
(O4.6) Protection strategy blueprint
(O5.1) Physical configuration of the information infrastructure
(O5.6) High-priority infrastructure components
(O6.2) Existing policies and practices
(O6.3) Missing policies and practices
(O6.6) Vulnerabilities
(O8.1) Candidate mitigation approaches
(O8.2) Protection strategy
(O8.3) Security risk management plan
(O8.4) Risk management measurement information
(I8.1) Current knowledge of enterprise management,project, and technical staffs
(I8.2) Available funding
(I8.3) Available staff
(I1.5) Organizational data
(I1.6) Laws and regulations
(O7.1) Validated intrusion scenarios
(O7.2) Exposed assets
(O7.3) Impact of exposed assets
(O7.4) Threat probability
(O7.5) Risks
(O7.6) Prioritized list of risks
(I7.1) Current knowledge of enterprise staff
(O4.1) Asset Map
(O4.4) Risk Indicators
(O4.6) Protection strategy blueprint
(O5.6) High-priority infrastructure components
(O6.1) Filtered intrusion scenarios
(O6.3) Missing policies and practices
(O6.6) Vulnerabilities
Key
P4 Establish Security Requirements
P5 Map High Priority Information Assets to Information Infrastructure
P6 Perform Technology Vulnerability Evaluation
P7 Conduct Multi-Dimensional Risk Analysis
P8 Develop Protection Strategy
Input
Output
Boldface type indicates a final output of the process.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (LEAVE BLANK)

2. REPORT DATE
June 1999

3. REPORT TYPE AND DATES COVERED
Technical Report
June 1999

3. TITLE AND SUBTITLE
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
Framework, Version 1.0

5. FUNDING NUMBERS
C — F19628-95-C-0003

6. AUTHOR(S)
Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, William R. Wilson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

7. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-99-TR-017
ESC-TR-99-017

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12.A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12.B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) is a framework for identifying and managing information security risks. It defines a comprehensive evaluation method that allows an organization to identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. With this understanding, the organization can design and implement a protection strategy to reduce the overall risk exposure of its information assets.

14. SUBJECT TERMS
information security, risk evaluation, risk assessment, threat analysis, vulnerability evaluation, network security, computer security

15. NUMBER OF PAGES
81

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL